会計検査院法第30条の2の規定に基づく報告書

「各府省庁等の情報システムに係る情報セキュリティ対策等の状況について」

令 和 ７ 年 ９ 月

会 計 検 査 院

国の行政機関等が実施する業務においては、情報システムの利用が拡大している。

また、インターネット等の高度情報通信ネットワークの整備等に伴ってサイバーセキュリティに対する脅威が世界規模で生じ、深刻化するなどしていることから、サイバーセキュリティを確保することにより、情報システムにおける情報セキュリティを確保することが重要となっている。そして、国のサイバーセキュリティに関する施策は、サイバーセキュリティ戦略本部、国家サイバー統括室（令和7年6月30日以前は内閣官房内閣サイバーセキュリティセンター）、デジタル庁等により推進されている。

一方、国の行政機関等においても、情報セキュリティインシデントが発生しており、情報セキュリティ対策等に関する取組の推進がより一層求められている。

本報告書は、以上のような状況を踏まえて、各府省庁等の情報システムに係る情報セキュリティ対策等の状況について検査し、その状況を取りまとめたことから、会計検査院法（昭和22年法律第73号）第30条の2の規定に基づき、会計検査院長から衆議院議長、参議院議長及び内閣総理大臣に対して報告するものである。

令 和 7 年 9 月

会 計 検 査 院

目　次

・本文及び図表中の数値は、原則として、表示単位未満を切り捨てているため、数値を集計しても計が一致しないものがある。
・図表中の「0」は単位未満あり、「-」は皆無を示す。
・図表は、本報告書の取りまとめに当たって会計検査院が作成したものである。

事 例 一 覧

各府省庁等の情報システムに係る情報セキュリティ対策等の状況について

検　査　対　象	(1) 内閣、内閣府、デジタル庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省及び防衛省の本府省庁等24機関 (2) 地方支分部局16機関
対象システムの概要	各府省庁等が整備、運用等を行っている情報システムのうち、様々な状況において重要な業務を実施するための情報システム
対象システム数	(1) 236システム (2) 120システム
対象システムの整備、運用等に係る経費の支払額	(1) 8439億7577万円　（令和3年度～5年度） (2)　362億1604万円　（令和3年度～5年度）

1　検査の背景

(1) 国のデジタル社会の実現に向けた取組の概要

政府は、「デジタル社会の実現に向けた改革の基本方針」（令和2年12月閣議決定。以下「改革基本方針」という。）において、デジタル社会の将来像等についての政府としての方針を示している。

改革基本方針によれば、行政において人的資源を行政サービスの更なる向上につなげられるようデジタル化を推進することで、行政の簡素化、効率化及び透明性の向上を図ることとされ、官民を含む社会全体でのデジタル化を円滑に進めていくためにも行政のデジタル化は緊要であるとされている。

このようなことから、国の行政機関等が実施する業務において、情報システム(注1)の利用が拡大している。

（注1）　情報システム　　ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するもの

(2) 国の情報セキュリティ対策の概要等

ア　国の情報セキュリティ対策に係る制度の概要等

インターネット等の高度情報通信ネットワークの整備等に伴ってサイバーセキュ

（注2）
リティに対する脅威が世界規模で生じ、深刻化するなどしていることから、サイバ
（注3）
ーセキュリティを確保することにより、情報システムにおける情報の機密性、
（注4）　（注5）
完全性及び可用性を維持すること（以下「情報セキュリティ」という。）が重要となっている。また、デジタル社会形成基本法（令和3年法律第35号）等に基づき策定された「デジタル社会の実現に向けた重点計画」（令和5年6月閣議決定。以下「重点計画」という。）によれば、政府は、自然災害により国民の生命・身体・財産に重大な被害が生じ、又は生ずるおそれがある事態を想定してサイバーセキュリティの確保等の取組を推進することとされている。

そして、サイバーセキュリティに関する施策を総合的かつ効果的に推進することなどを目的として「サイバーセキュリティ基本法」（平成26年法律第104号。以下「法」という。）が制定されている。法に基づき定められた「サイバーセキュリティ戦略」（令和3年9月閣議決定）によれば、国の行政機関等は、サイバーセキュリティ対策を進め、情報システムの開発・構築段階も含めたあらゆるフェーズでの対策を強化していくこととされている。また、国民の安全・安心の根幹に関わる経済社会基盤の防護については、これを担う国の行政機関等が役割に応じて情報セキュリティを確実に保証することとされている。

国の行政機関等は、法等に基づくなどして、サイバーセキュリティ対策を含む情報セキュリティ対策の強化・拡充を図っており、国のサイバーセキュリティに関する施策は、図表0-1のとおり、内閣に設置されたサイバーセキュリティ戦略本部（以下「本部」という。）、内閣官房に設置された内閣サイバーセキュリティセンター
（注6）
（以下「ＮＩＳＣ」という。令和7年7月1日以降は国家サイバー統括室）、デジタル庁等により推進されている。

（注2）　サイバーセキュリティ　電子的方式等により記録される情報の漏えい、滅失又は毀損の防止等の安全管理のために必要な措置並びに情報システム等の安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること

（注3）　機密性　情報に関して、アクセスを認められた者だけがこれにアクセスできる特性のこと

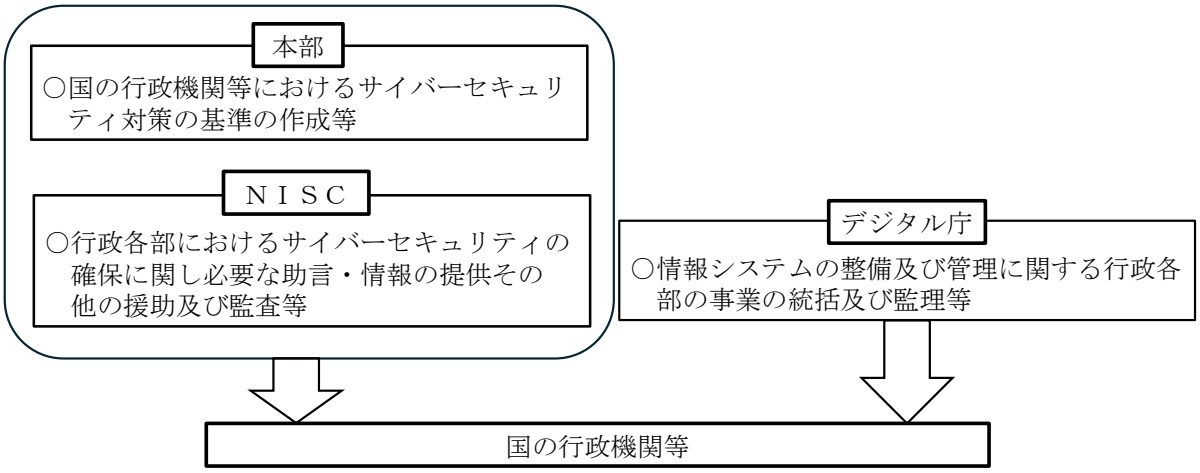
（注4）　完全性　情報が破壊、改ざん又は消去されていない特性のこと

（注5）　可用性　情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性のこと

（注6）　国家サイバー統括室は、「国家安全保障戦略」（令和4年12月閣議決定）に基づき、サイバー安全保障分野の政策を一元的に総合調整する新たな組

織としてＮＩＳＣを改組して設置されたものである。

図表0-1　本部、ＮＩＳＣ及びデジタル庁の役割



本部、ＮＩＳＣ及びデジタル庁が担う役割の詳細は次のとおりとなっている。

(ｱ) 本部及びＮＩＳＣ

法によれば、本部は、国の行政機関等におけるサイバーセキュリティ対策の基準の作成、当該基準に基づく施策の評価（監査を含む。）等を行うこととされている。

また、本部に関する事務は内閣官房において処理することとされており、内閣官房に設置されたＮＩＳＣが、①行政各部におけるサイバーセキュリティの確保に関し必要な助言・情報の提供その他の援助及び監査、②行政各部の施策に関する統一保持上必要な企画及び立案並びに総合調整に関する事務のうちサイバーセキュリティの確保に関する事務（国家安全保障局等において行うものを除く。）等を行っている。

(ｲ) デジタル庁

デジタル庁設置法（令和3年法律第36号）によれば、デジタル庁は、国の行政機関が行う情報システムの整備及び管理に関する行政各部の事業を統括し及び監理することとされており、政府情報システム(注7)のサイバーセキュリティ対策等を実践するための参考となるガイドライン等の策定を行うなどしている。

（注7）　政府情報システム　　各府省庁等がサービス・業務を実施するために用いる情報システム

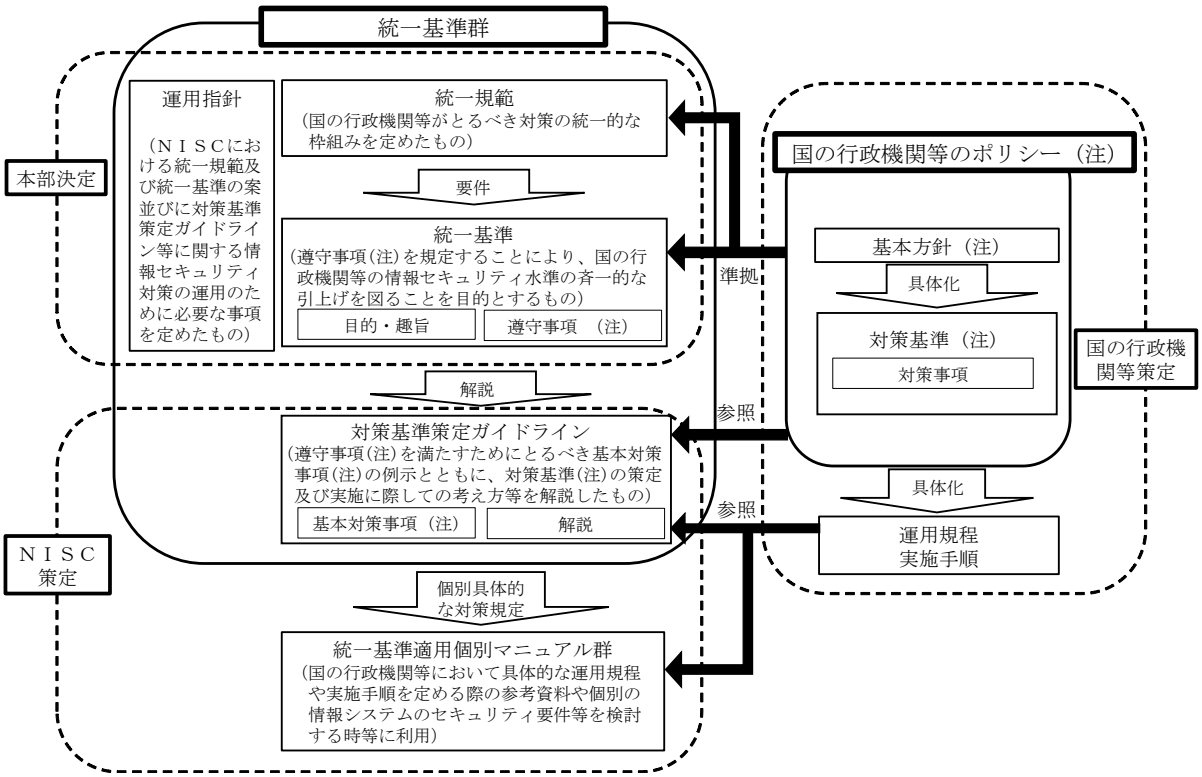
イ　統一基準群の体系の概要等

(ｱ) 統一基準群の体系の概要

本部は、国の行政機関等が自らの責任において講ずべきサイバーセキュリティ対策の基準として、図表0-2のとおり、「政府機関等のサイバーセキュリティ対策のための統一規範」（平成28年8月決定。以下「統一規範」という。）、「政府機関等のサイバーセキュリティ対策のための統一基準」（平成17年12月決定。以下「統一基準」という。）及び「政府機関等のサイバーセキュリティ対策の運用等に関する指針」（平成28年8月決定。以下「運用指針」という。）を定めている。

また、ＮＩＳＣは、「政府機関等の対策基準策定のためのガイドライン」（平成17年12月決定。以下「対策基準策定ガイドライン」といい、統一規範、統一基準、運用指針及び対策基準策定ガイドラインを合わせて「統一基準群」という。）等を定めている。

図表0-2　統一基準群の体系等



（注）「遵守事項」「基本対策事項」「ポリシー」「基本方針」及び「対策基準」については、後述エ(ｱ)参照

(ｲ) 統一基準における情報セキュリティ対策の概要

統一基準においては、図表0-3のとおり、国の行政機関等において共通的に必要とされる情報セキュリティ対策の項目が八つの部に区分して定められている。

図表0-3　統一基準における情報セキュリティ対策の項目

部	情報セキュリティ対策の項目
第1部　総則	統一基準の目的・適用範囲等
第2部　情報セキュリティ対策の基本的枠組み	組織・体制の整備、対策基準・対策推進計画の策定、教育、情報セキュリティ監査、情報セキュリティ対策の見直し等
第3部　情報の取扱い	情報の取扱い、情報を取り扱う区域の管理
第4部　外部委託	業務委託、外部サービスの利用
第5部　情報システムのライフサイクル	情報システムに係る台帳等の整備、情報システムの運用継続計画の整備・整合的運用の確保等
第6部　情報システムのセキュリティ要件	主体認証（注(2)）機能、アクセス制御機能、権限の管理、ログ（注(3)）の取得・管理、ソフトウェアに関するぜい弱性対策等
第7部　情報システムの構成要素	端末・サーバ装置等
第8部　情報システムの利用	情報システムの利用等

注(1)　下線部分は「3　検査の状況」において記述している項目である。
注(2)　「主体認証」は、主体（情報システム等にアクセスする者等）が、正当であるか否かを検証することである。
注(3)　「ログ」は、システムの動作履歴、利用者のアクセス履歴、通信履歴その他運用管理等に必要な情報を記録したデータである。

(ｳ) 統一基準群の改定の概要

統一基準群は、サイバーセキュリティを取り巻く情勢の変化等に応じて、おおむね2年に一度、改定が行われている。そして、ＮＩＳＣは、情報セキュリティに関する動向を踏まえ、国の行政機関等の全体に関わるサイバーセキュリティ対策のうち改善等が必要と考えられる項目について行った調査や、法に基づき行った監査の結果を、統一基準群の改定等に反映させている。

ウ　標準ガイドライン群等の概要

政府は、政府情報システムの整備及び管理について、体系的な政府共通のルールを定めた「デジタル・ガバメント推進標準ガイドライン」（平成26年12月各府省情報化統括責任者（ＣＩＯ）連絡会議決定。以下「標準ガイドライン」という。）を策定している。

また、デジタル庁は、標準ガイドラインの趣旨、目的等を理解しやすくするための「デジタル・ガバメント推進標準ガイドライン解説書」（平成31年2月決定）等（以下、標準ガイドラインと合わせて「標準ガイドライン群」という。）を定めている。

そして、デジタル庁は、標準ガイドライン群等に基づき、政府情報システムの整備及び管理に関する事業を特定して、より適切な管理等を実施するために、予算要求前から執行の段階までを含むプロジェクト監理の一環として、各政府情報システ

ムに情報システムＩＤを付番している。

エ　国の行政機関等における情報セキュリティ対策の概要

国の行政機関等は、統一基準群及び標準ガイドライン群に基づき、次のような情報セキュリティ対策を講じている。

(ｱ) 統一基準群に基づく情報セキュリティ対策の概要

a　ポリシー等の策定

統一基準群によれば、国の行政機関等は、自組織の特性を踏まえ、情報セキュリティ対策の基本的な方針（以下「基本方針」という。）及び情報セキュリティ対策の基準（以下「対策基準」といい、基本方針及び対策基準を合わせて「ポリシー」という。）を定めなければならないこととされている。そして、統一基準群においては、情報セキュリティ対策の項目ごとに遵守すべき事項（以下「遵守事項」という。）や、国の行政機関等が遵守事項を満たすためにとるべき基本的な対策事項（以下「基本対策事項」という。）が定められている。

そして、国の行政機関等は、遵守事項等の規定を満たすように、具体的な対策事項を対策基準に規定した上で、これに基づいて運用規程や実施手順のセキュリティ関係規程を定めることにより、基本対策事項に例示される対策又はこれと同等以上の対策を講ずる必要があるとされている（統一基準群とポリシーとの関係は図表0-2参照）。

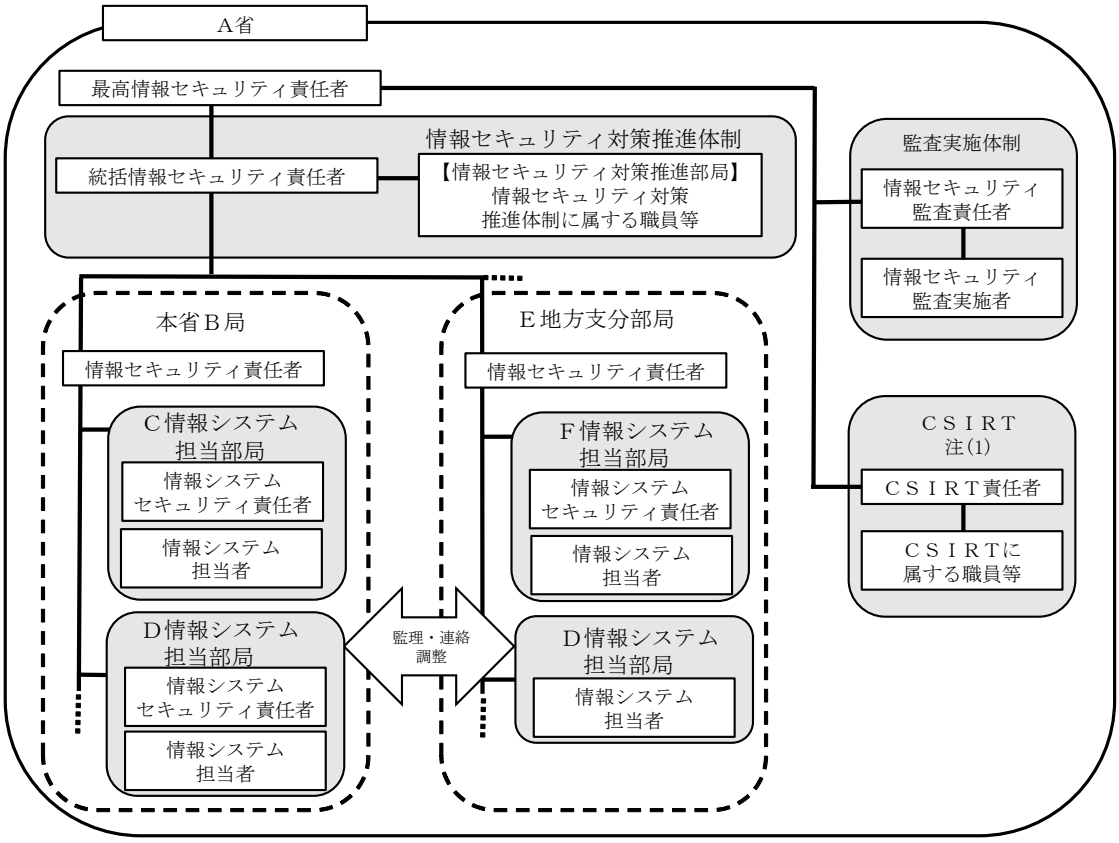
b　情報セキュリティ監査

統一基準群によれば、国の行政機関等は、対策基準が統一規範及び統一基準に準拠し、かつ実際の運用が対策基準に準拠していることを確認するために情報セキュリティ監査を行わなければならないこととされている。そして、情報セキュリティ監査の結果等を勘案して、情報システムに係るリスクを評価し、必要な情報セキュリティ対策を講じなければならないこととされている。

c　組織体制

国の行政機関等は、統一基準群に基づき、情報セキュリティ対策の推進に係る事務を遂行するための体制（以下「情報セキュリティ対策推進体制」という。）等を整備している（図表0-4参照）。

図表0-4　国の行政機関等における情報セキュリティ対策推進体制等の例



注(1)　「ＣＳＩＲＴ」については、後述注12参照
注(2)　対策基準策定ガイドラインを基に会計検査院が作成した。

国の行政機関等は、統一基準群に基づき、情報セキュリティに関する事務を統括する最高情報セキュリティ責任者及び同責任者の補佐等を行う統括情報セキュリティ責任者を置いている。そして、各情報システムについて担当部局を決めているほか、基本的に情報システムごとに情報システムセキュリティ責任者及び情報システム担当者を置いている。

また、最高情報セキュリティ責任者は、監査に関する事務を統括する者として情報セキュリティ監査責任者を置くこととされており、情報セキュリティ監査責任者は、監査実施計画の策定、監査の実施指示、監査結果の最高情報セキュリティ責任者への報告等の事務を統括することとされている。(注8)

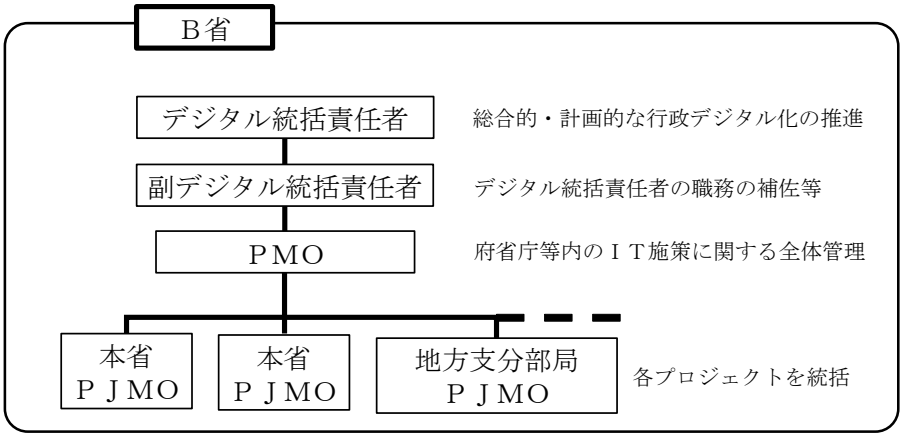
(注8)　最高情報セキュリティ責任者、統括情報セキュリティ責任者、情報セキュリティ監査責任者等は、各府省等に設置されているものとは別に、各府省の外局である庁に設置されている場合等があり、設置されている府省庁等を単位として取組が実施されている。

(ｲ) 標準ガイドライン群に基づく情報セキュリティ対策の概要

各府省庁等は、標準ガイドライン群に基づき、各府省庁等における行政デジタ

ル化全体の管理体制として、図表0-5のとおり、デジタル統括責任者及び副デジタル統括責任者のほか、府省庁等内のＩＴ施策に関する全体管理の機能を担う組織であるＰＭＯ（Portfolio Management Office）や、各プロジェクトを統括する組織であるＰＪＭＯ（ProJect Management Office）を設置している。そして、このうち、ＰＪＭＯについては、情報システム部門の職員だけでなく、業務実施部門等の職員も適切に参画するように組織することとなっている。

図表0-5　各府省庁等における行政デジタル化全体の管理体制の例



（注）　標準ガイドラインを基に会計検査院が作成した。

標準ガイドラインによれば、ＰＪＭＯは、政府情報システムの整備及び管理に係るプロジェクトの実施に当たり、調達仕様書等において、政府情報システムに求める要件を定めることとされている。そして、当該要件として、情報システムの運用の継続性（障害、災害等による情報システムの問題発生時に求められる機能、システム構成等）や、情報システムの情報セキュリティ対策に関する事項を定めることとされている。また、ＰＪＭＯは、原則として、情報システムの運用時において、情報セキュリティ対策等の事項についてＰＭＯ等と調整することとされている。

オ　ＩＴ－ＢＣＰの概要

「政府業務継続計画（首都直下地震対策）」（平成26年3月閣議決定。以下「政府業務継続計画」という。）によれば、各府省庁等は、「政府機関等における情報システム運用継続計画ガイドライン（第3版）」（令和3年4月内閣官房内閣サイバーセキュリティセンター作成。以下「ＩＴ－ＢＣＰガイドライン」という。）に基づき情報システム運用継続計画を策定することとされている（以下、ＩＴ－ＢＣＰガイ

ドラインに基づき策定された情報システム運用継続計画を「ＩＴ－ＢＣＰ」という。）。

ＩＴ－ＢＣＰは、危機的事象(注9)が発生して、情報システムの運用が中断し又は途絶するときに、情報システムを継続し又は復旧させることにより、その影響を最小限に抑えるために必要な計画群の総称であり、危機的事象発生時にＩＴ－ＢＣＰに沿って適切に対処することは、情報システム担当者の重要な役割の一つとなっている。

（注9）　危機的事象　　不正アクセス等の運用妨害、地震等の自然災害、火災等の人的災害等の様々な事象

(3) 政府デジタル人材の確保・育成等の概要

重点計画によれば、各府省庁等は、情報システムの整備・運用に当たり、委託業者任せにするのではなく、専門人材の採用等によって行政機関内部の体制を整備し、自らプロジェクトを適切に推進して管理することとされている。また、各府省庁等は、情報システムの適切な開発・運用やサイバーセキュリティ対策等の担い手となる人材を充実させるなどの政府デジタル人材の確保・育成等の取組を推進することとされている。

そして、「政府機関におけるデジタル改革に必要なＩＴ・セキュリティ知識を有する人材の確保・育成総合強化方針」（令和3年7月サイバーセキュリティ対策推進会議（ＣＩＳＯ等連絡会議）・各府省情報化統括責任者（ＣＩＯ）連絡会議決定）によれば、各府省庁等は、所定の研修を修了した者について、業務経験も踏まえたスキル認定を行うこととされており、そのための共通の基準として、「政府デジタル人材のスキル認定の基準」（平成30年1月サイバーセキュリティ対策推進専任審議官等会議・各府省情報化専任審議官等会議合同会議決定）が定められている。

(4) ＮＩＳＣ等における情報セキュリティ対策に関する取組の概要

ア　法に基づく監査

ＮＩＳＣは、法に基づく監査として、国の行政機関等における統一基準群等に基づく施策の取組状況等について検証するなどの監査（以下「マネジメント監査」という。）や、擬似的な攻撃により実際に情報システムに侵入できるかどうかの観点からサイバーセキュリティ対策の状況を検証するなどの監査を実施して、サイバーセキュリティ対策を改善するための助言等を行うことで、国の行政機関等におけるサイバーセキュリティ対策の強化を図っている。このうち、マネジメント監査の結

果は毎年公表されており、「サイバーセキュリティ2024（2023年度年次報告・2024年度年次計画）」（令和6年7月サイバーセキュリティ戦略本部決定）によると、情報システムのセキュリティ要件に関する指摘が多くなっている（マネジメント監査における指摘に係る統一基準の部別の割合等については別図表1参照）。

イ　クラウドサービスリストの公開

政府情報システムの整備及び管理に当たっては、オンプレミス(注10)からクラウド(注11)への移行が促されており、クラウドサービスの利用を第一候補として検討するクラウド・バイ・デフォルト原則に基づき調達を行うこととなっている。

そして、ＮＩＳＣ、デジタル庁等は、安全性が評価されたクラウドサービスを登録して公開することにより、情報セキュリティ対策が十分なクラウドサービスを各府省庁等が効率的に調達できるよう、政府情報システムのためのセキュリティ評価制度（以下「ＩＳＭＡＰ」という。）を運用している。ＩＳＭＡＰは、2年6月に運用が開始され、3年3月に初回となるクラウドサービスリストの登録及び公開が行われ、各府省庁等による利用が開始されている。

（注10）　オンプレミス　　アプリケーションごとに個別の動作環境（サーバ等）を準備して自ら運用する形態

（注11）　クラウド　　システムの整備、運用等の効率化を図るために、一元管理されたコンピュータ資源をネットワーク経由で利用する形態

ウ　教育・訓練

ＮＩＳＣは、国の行政機関等の情報セキュリティ対策推進体制に属する職員や情報システム担当者等を対象として、統一基準群やマネジメント監査の結果等についての講義を実施する勉強会(注12)（以下「ＮＩＳＣ勉強会」という。）、ＣＳＩＲＴ要員を対象とした研修訓練等を実施している。

（注12）　ＣＳＩＲＴ　　Computer Security Incident Response Teamの略。組織内において発生した情報セキュリティインシデント（後述注13参照）に対処するために、当該組織内に設置された体制

(5) 情報セキュリティインシデントの発生状況

本部が3年度から5年度までに公表している年次計画及び年次報告によると、本部が国の行政機関等から受けた情報セキュリティインシデント(注13)に関連する報告等の件数は、3年度207件、4年度266件、5年度233件となっている。そして、これらの情報セキュリティインシデントの主な要因は、「外部からの攻撃」と、関係のない第三者へ誤ってメールを送信した事案等に係る「意図せぬ情報流出」となっている（国の行政機関等

が公表している主な情報セキュリティインシデントについては別図表2参照）。

（注13）　情報セキュリティインシデント　　望まない又は予期しない情報セキュリティ事象であって、事業運営を危うくする又は情報セキュリティの確保に脅威を及ぼす可能性のある事象

(6) これまでの検査の実施状況

会計検査院は、これまで、各府省庁等における情報セキュリティ対策や情報システムの運用の継続性の状況について検査し、その結果を検査報告に掲記するなどしている（別図表3参照）。

2　検査の観点、着眼点、対象及び方法

(1) 検査の観点及び着眼点

国の行政機関等が実施する業務においては、情報システムの利用が拡大している。

また、インターネット等の高度情報通信ネットワークの整備等に伴ってサイバーセキュリティに対する脅威が世界規模で生じ、深刻化するなどしていることから、サイバーセキュリティを確保することにより、情報システムにおける情報セキュリティを確保することが重要となっている。そして、国のサイバーセキュリティに関する施策は、本部、ＮＩＳＣ、デジタル庁等により推進されている。

一方、国の行政機関等においても、情報セキュリティインシデントが発生しており、情報セキュリティ対策等に関する取組の推進がより一層求められている。

そこで、会計検査院は、合規性、効率性、有効性等の観点から、各府省庁等の情報システムに係る情報セキュリティ対策等の状況について、次の点に着眼するなどして検査した。

ア　情報システムの整備、運用等に係る経費の支払状況及び契約の状況はどのようになっているか。

イ　情報システムに係る情報セキュリティ対策は、統一基準群等に基づき適切に講じられているか。(注14)

ウ　情報セキュリティ対策に係る教育等及び監査は、統一基準群等に基づき適切に実施されているか。(注14)

（注14）　統一基準群は、令和3年7月に改定された後、5年7月及び7年7月にも改定されているが、3年度から5年度までの状況を検査の対象としていることを踏まえて、3年7月改定時点の統一基準群の規定であって、5年7月及び7年7月の改定後の統一基準群においても同様に定められているものなどに基づいて検査した。

(2) 検査の対象及び方法

会計検査院は、6年3月末時点において14府省庁等(注15)の本府省庁等(注16)24機関が整備、運用等を行っている情報システム(注17)のうち、様々な状況において重要な業務を実施するための情報システム（以下「対象システム」という。）236システム、及び14府省庁等の地方支分部局のうち16機関が整備、運用等を行っている対象システム120システムに係る情報セキュリティ対策等の状況について、3年度から5年度までを対象として検査した。

検査に当たっては、本府省庁等24機関及び地方支分部局16機関において、契約書、調達仕様書等の関係資料を確認するとともに、内閣官房及びデジタル庁においては、

ＮＩＳＣ及びデジタル庁が実施しているサイバーセキュリティに関する施策等の状況についても関係資料を確認するなどして会計実地検査を行ったほか、24機関及び16機関から調書の提出を受けてその内容を分析するなどして検査した。

なお、ＮＩＳＣを改組して設置された国家サイバー統括室は、各対象システムに係る情報セキュリティ対策等の状況に関する詳細な事実関係や、会計検査院が具体的にどのような情報システムを検査の対象としたのかなどの情報が公開された場合、特定の対象システムにおける情報セキュリティ対策等の問題点を狙い撃ちにした攻撃を誘発するなどのリスクがあるため、サイバーセキュリティを確保する観点から公開すべきではないとしている。

上記を踏まえて、これらの情報については、本報告書には記述しないこととした。

（注15）　14府省庁等　　内閣、内閣府、デジタル庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省

（注16）　24機関　　内閣官房、内閣府、警察庁、金融庁、消費者庁、こども家庭庁、デジタル庁、総務省、消防庁、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、資源エネルギー庁、国土交通省、気象庁、海上保安庁、環境省及び防衛省の本府省庁、国土地理院及び原子力規制委員会

（注17）　国の行政機関等が調達又は開発した情報システムであって、管理を外部の業者に委託している情報システムを含む。

3　検査の状況

(1) 対象システムの整備、運用等に係る経費の支払状況及び契約の状況

対象システムについては、情報システムの整備に必要なハードウェア又はソフトウェアの調達、情報システムの運用等に必要な役務の調達等の様々な内容の契約が締結され、これらの契約に基づき整備、運用等に係る経費が支払われている。そして、情報システムの整備、運用等に係る経費には、情報セキュリティ対策に係る経費が含まれている。(注18)

一方、会計検査院は、参議院から国会法（昭和22年法律第79号）第105条の規定に基づく検査要請を受けて、その検査結果を3年5月に「政府情報システムに関する会計検査の結果について」として報告している（以下、この報告を「3年報告」という。）。そして、3年報告においては、政府情報システムに関する予算の執行状況、契約の状況等についての検査結果を記述している。

そこで、対象システムの整備、運用等に係る経費の支払状況及び契約の状況についてみたところ、次のとおりとなっていた。

（注18）　情報システムの整備、運用等に係る経費のうち、情報セキュリティ対策に係る経費とその他の経費は、多くの場合に切り分けが困難である。

ア　経費の支払状況

本府省庁等24機関が3年度から5年度までに整備、運用等に係る経費を支払った対象システムは、図表1-1のとおり、224システムであり、当該支払に係る契約の件数は2,875件となっていた。また、支払われた経費の額は計8439億7577万余円であり、このうち整備経費(注19)は2921億9988万余円、運用等経費(注20)は5517億7589万余円となっていた。

また、地方支分部局16機関が3年度から5年度までに整備、運用等に係る経費を支払った対象システム(注21)は128システムであり、当該支払に係る契約の件数は658件となっていた。また、支払われた経費の額は計362億1604万余円であり、このうち整備経費は154億3140万余円、運用等経費は207億8464万余円となっていた。

（注19）　整備経費　　情報システムの整備（新規開発、機能改修・追加、更改及びこれらに付随する環境の整備）に要する一時的な経費

（注20）　運用等経費　　情報システムの運用、保守等に要する経常的な経費

（注21）　本府省庁等の対象システムの中には、地方支分部局が利用していて、地方支分部局が整備、運用等に係る経費の支払を行った対象システムがあるため、地方支分部局の対象システム数（120システム）を上回っている。

図表1-1　本府省庁等24機関における対象システムの整備、運用等に係る経費の支払状況及び契約の状況（令和3年度～5年度）

（単位：件、千円）

番号	機関名	対象システム数	左のうち経費の支払を行った対象システム数 注(1)	契約件数 注(1)	支払額 注(1)		
					整備経費 注(2)	運用等経費 注(2)	計
1	内閣官房	4	4	35	1,409,840	3,529,569	4,939,410
2	内閣府本府	6	6	37	1,252,020	1,798,413	3,050,434
3	警察庁	35	31	249	35,273,224	40,078,439	75,351,663
4	金融庁	4	4	179	994,860	4,041,806	5,036,667
5	消費者庁	1	1	1	－	153,010	153,010
6	こども家庭庁	1	1	2	3,203	－	3,203
7	デジタル庁	9	9	247	37,829,901	97,350,079	135,179,980
8	総務本省	4	4	69	8,950,575	3,738,468	12,689,044
9	消防庁	11	11	72	1,955,652	2,402,897	4,358,549
10	法務本省	10	10	279	31,849,527	73,235,276	105,084,804
11	外務本省	21	18	409	15,493,805	34,993,262	50,487,068
12	財務本省	15	15	229	23,894,847	56,107,594	80,002,441
13	文部科学本省	3	3	6	－	7,000,642	7,000,642
14	厚生労働本省	8	8	77	1,778,194	28,017,864	29,796,059
15	農林水産本省等	2	2	12	51,430	189,086	240,517
16	経済産業本省	2	2	7	－	11,284,570	11,284,570
17	資源エネルギー庁	1	1	2	－	37,777	37,777
18	国土交通本省	34	29	213	81,535,405	39,874,046	121,409,452
19	国土地理院	6	6	58	1,238,091	743,684	1,981,776
20	気象庁本庁	24	24	230	24,214,632	10,056,205	34,270,838
21	海上保安庁本庁	16	16	155	9,267,364	7,638,950	16,906,315
22	環境本省	5	5	41	5,361,998	1,480,761	6,842,759
23	原子力規制委員会	6	6	72	5,830,639	5,962,943	11,793,582
24	防衛本省	8	8	194	4,014,668	122,060,541	126,075,209
計		236	224	2,875	292,199,885	551,775,890	843,975,776

注(1)　「左のうち経費の支払を行った対象システム数」は、24機関が、令和3年度から5年度までに整備、運用等に係る経費を支払った対象システム数を記載しており、「契約件数」は当該支払に係る契約の件数を、「支払額」は当該支払の額をそれぞれ記載している。

注(2)　一つの契約により整備経費と運用等経費の両方が支払われている場合は、当該契約の主たる内容に基づいて整備経費と運用等経費のいずれかに支払額の全額を計上している。

イ　契約の状況

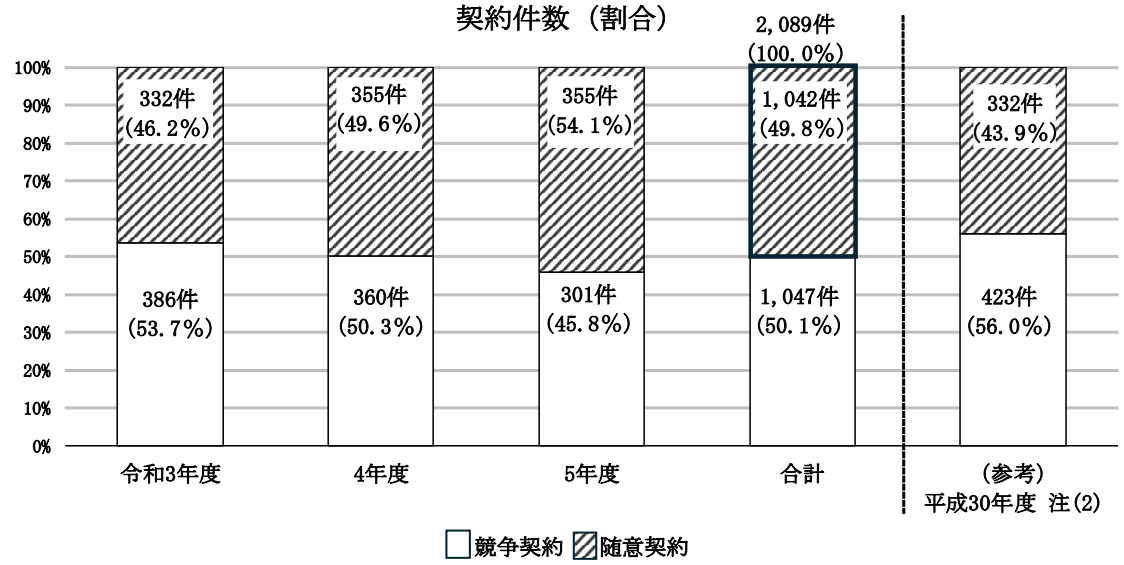
(ｱ) 契約方式の状況

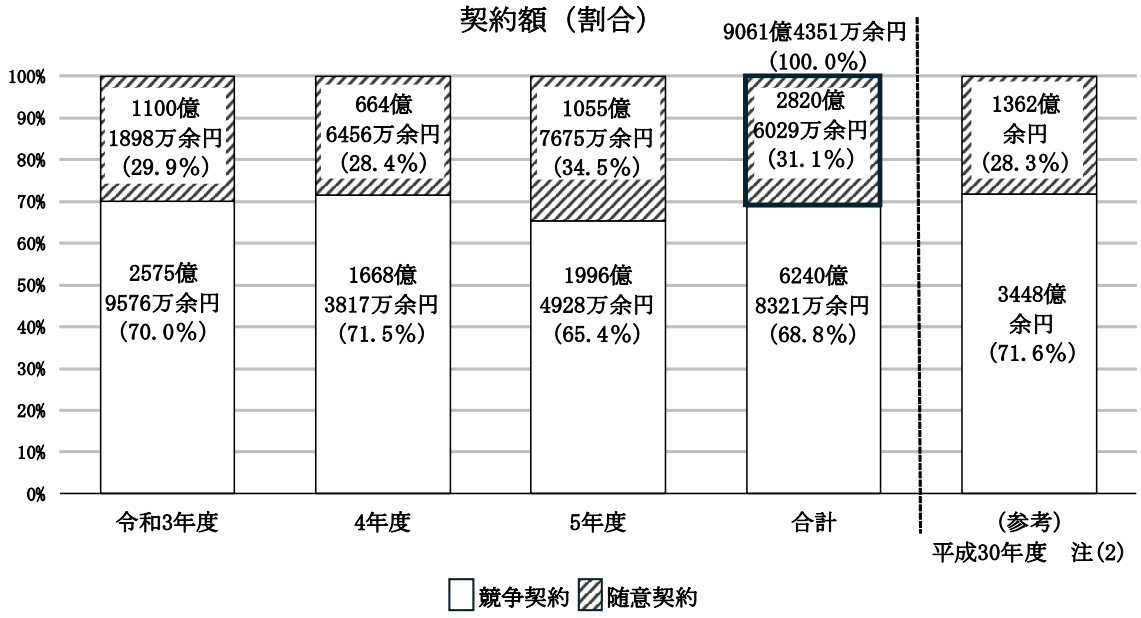
会計法（昭和22年法律第35号）、予算決算及び会計令（昭和22年勅令第165号）等によれば、国が契約を締結する場合、原則として競争に付さなければならないこととされている。ただし、契約に係る予定価格が少額である場合のほか、契約の性質又は目的が競争を許さない場合等は随意契約によることができるとされている（以下、予定価格が少額であることを理由とした随意契約を「少額随契」という。）。そして、「予算決算及び会計令及び予算決算及び会計令臨時特例の一部を改正する政令」（令和7年政令第93号。以下「改正令」という。）による改正前は、①予定価格が250万円を超えない工事又は製造をさせるとき、②予定価格が160万円を超えない財産を買い入れるとき、③工事又は製造の請負、財産の売買及

び物件の貸借以外の契約でその予定価格が100万円を超えないものであるときなどは少額随契によることができるとされていた。

そこで、本府省庁等24機関が3年度から5年度までに契約の締結及び経費の支払を行っている契約のうち、契約額（単価契約の場合は、調達時の想定数量に契約単価を乗じた額）が少額随契によることができる予定価格の額を超えている契約2,089件（契約額計9061億4351万余円）の契約方式について確認した。その結果、特定の者でなければ履行することができないことから、契約の性質又は目的が競争を許さない場合に該当するなどとして随意契約により締結していた契約は、図表1-2のとおり、1,042件（2,089件の49.8%）で、契約額は2820億6029万余円（9061億4351万余円の31.1%）となっていた。

図表1-2　契約方式別の契約件数及び契約額（令和3年度～5年度）





注(1)　各年度の契約件数及び契約額は、各年度に締結された契約について集計しており、国庫債務負担行為による複数年度契約の契約額については、当初契約を締結した年度に契約額の全額を計上している。
注(2)　3年報告においては、平成30年度に締結した政府情報システムの整備、運用等に係る契約であって、契約額が3000万円以上の契約件数及び契約額を集計して記載していることから、単純な比較はできないが、参考として当該契約件数及び契約額を記載している。

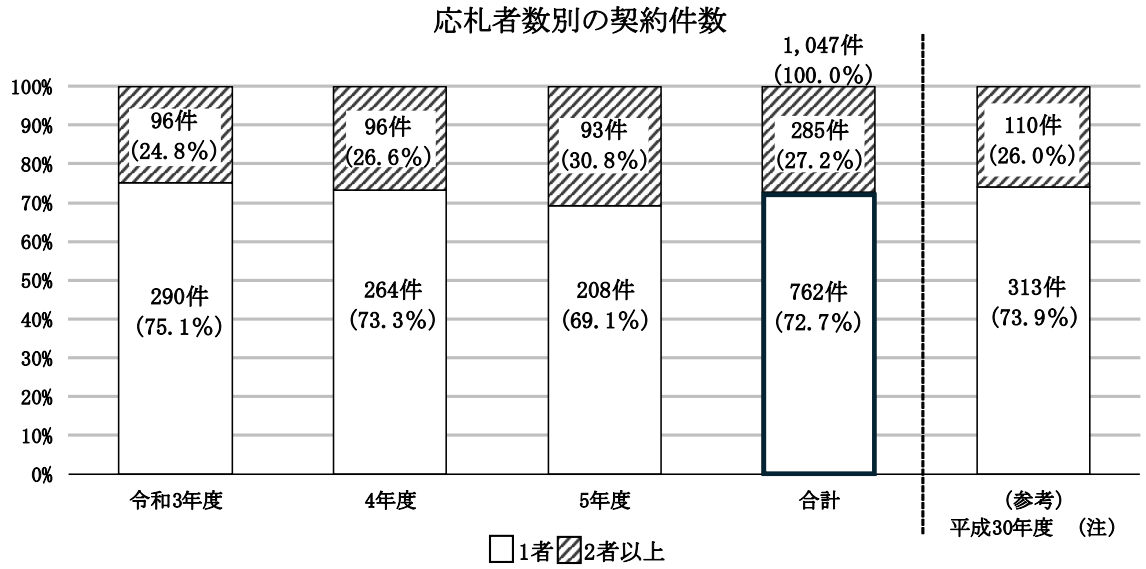
(ｲ) 競争契約における1者応札の状況

競争契約に当たっては、できるだけ多くの入札者の参加により実質的な競争性が確保されていることが重要である。

そこで、本府省庁等24機関が3年度から5年度までに契約の締結及び経費の支払を行っている契約のうち競争契約により締結された契約1,047件における応札者数

を確認したところ、図表1-3のとおり、応札者が1者であった契約（以下「1者応札」という。）の件数は762件（1,047件の72.7%）となっていた（競争契約の応札者数別の契約件数及び契約額については別図表4参照）。

図表1-3　競争契約の応札者数別の契約件数（令和3年度～5年度）



（注）　3年報告においては、平成30年度に締結した政府情報システムの整備、運用等に係る契約であって、契約額が3000万円以上の契約について、競争契約の応札者数別の契約件数を集計して記載していることから、単純な比較はできないが、参考として当該契約件数を記載している。

また、5年度の1者応札208件のうち、当該契約の受注者が3年度及び4年度にも同様の内容の契約を1者応札により受注しているもの（以下「継続受注」という。）は、図表1-4のとおり、69件（208件の33.1%）となっていた。そして、整備経費に係る契約と運用等経費に係る契約を比較すると、運用等経費に係る契約の方が継続受注となっている件数の割合が高くなっていた。

図表1-4　継続受注の状況

（単位：件）

経費の種類	1者応札の契約 （令和5年度） a	うち継続受注の契約 注(1)、注(2)、注(3) b	割合 b/a
整備経費	86	16	18.6%
運用等経費	122	53	43.4%
計	208	69	33.1%

注(1)　年度の途中で契約が分かれている場合（令和3年度前期分と同年度後期分等）には、同一の者が当該年度の全ての契約を1者応札により受注していれば、集計の対象としている。

注(2)　更改前のシステムに係る保守契約と更改後のシステムに係る保守契約については、同様の内容の契約として集計している。

注(3)　ソフトウェアのライセンス等の購入や年度の途中で発注する追加業務に係る契約、及び国庫債務負担行為により契約期間が複数年度にわたる契約は、集計の対象としていない。

(2) 対象システムに係る情報セキュリティ対策の実施状況等

1(2)イ(ｲ)のとおり、統一基準においては、国の行政機関等において共通的に必要とされる情報セキュリティ対策の項目が部に区分して定められている（図表0-3参照）。

そこで、統一基準に基づき、対象システム（本府省庁等24機関の236システム及び地方支分部局16機関の120システム）に係る情報セキュリティ対策が適切に講じられているかなどについて確認したところ、各機関において統一基準群に準拠した運用を行う必要があることについての認識が欠けていたこと、基本対策事項についての理解が十分でなかったことなどのため、情報セキュリティ対策が適切に講じられていないなどの状況が見受けられた（図表2-1参照）。

図表2-1　情報セキュリティ対策が適切に講じられていないなどの状況

部	情報セキュリティ対策が適切に講じられていないなどの状況が見受けられた項目　（注）
第2部　情報セキュリティ対策の基本的枠組み	・情報セキュリティ対策の見直し（ア(ｲ)）
第4部　外部委託	・業務委託（ウ(ｱ)） ・外部サービスの利用（ウ(ｲ)）
第5部　情報システムのライフサイクル	・情報システムに係る台帳等の整備（ア(ｱ)） ・情報システムの運用継続計画の整備・整合的運用の確保（イ(ｵ)）
第6部　情報システムのセキュリティ要件	・主体認証機能（イ(ｳ)） ・権限の管理（イ(ｲ)） ・ログの取得・管理（イ(ｴ)） ・ソフトウェアに関するぜい弱性対策（イ(ｱ)）

（注）　本報告書の記載箇所を括弧書きで記載している。

これらの情報セキュリティ対策が適切に講じられていないなどの状況は、アからウ

までのとおりである。

ア　対象システムに係る台帳の整備状況等

(ｱ) 情報システム台帳の整備状況

統一基準群によれば、統括情報セキュリティ責任者は、情報システム台帳を整備することとされている。また、情報システムセキュリティ責任者は、情報システムを新たに整備する際等には、当該情報システムのセキュリティ要件に係る内容を情報システム台帳に記載して、統括情報セキュリティ責任者に報告することとされている。そして、情報システム台帳に記載するセキュリティ要件に係る内容として、情報システムで取り扱う情報の格付(注22)等に関する事項等の12事項が定められている（情報システム台帳に記載する12事項については、別図表5参照）。

（注22）　情報の格付　　統一基準群によれば、機密性、完全性及び可用性の三つの観点に区別して、観点ごとに二つ又は三つの区分に分類することとされている。

a　情報システム台帳による管理

対象システムの情報システム台帳による管理状況を確認したところ、図表2-2のとおり、本府省庁等16機関の41システム（236システムの17.3%）及び地方支分部局10機関の56システム（120システムの46.6%）については、情報システム台帳に記載されておらず、情報システム台帳による管理が行われていなかった。

図表2-2　対象システムの情報システム台帳による管理状況（令和6年3月末時点）

機関	情報システム台帳による管理が行われている対象システム			情報システム台帳による管理が行われていない対象システム			計	
	機関数（注）	システム数		機関数（注）	システム数		機関数（注）	システム数
		a	割合 a/c		b	割合 b/c		c
本府省庁等	20	195	82.6%	16	41	17.3%	24	236
地方支分部局	13	64	53.3%	10	56	46.6%	15	120

（注）　整備、運用等を行っている対象システムの中に、情報システム台帳により管理しているものと管理していないものが含まれている機関があるため、機関数を集計しても計欄と一致しない。また、地方支分部局16機関のうち1機関は、他の地方支分部局が対象システムを管理しており、対象システムを利用しているのみであるため、機関数の計が15機関となっている。

b　セキュリティ要件に係る記載

情報システム台帳による管理が行われていた図表2-2の本府省庁等20機関の195システム及び地方支分部局13機関の64システムについて、情報システム台帳

におけるセキュリティ要件に係る内容の記載状況を確認したところ、図表2-3のとおり、本府省庁等13機関の109システム及び地方支分部局12機関の62システムについては、情報システム台帳に記載することとされている12事項のうち一部の事項が記載されていなかった。

また、情報システムに係る情報セキュリティ対策は、当該情報システムで取り扱う情報の格付等を踏まえて実施する必要があることなどから、12事項のうち取り扱う情報の格付に関する事項の情報システム台帳への記載状況を確認したところ、図表2-3のとおり、本府省庁等9機関の90システム及び地方支分部局12機関の62システムについては、機密性、完全性及び可用性の三つの観点による区分のうちのいずれかが記載されていなかった。

図表2-3　情報システム台帳におけるセキュリティ要件に係る内容の記載状況（令和6年3月末時点）

機関	項目	12事項が全て記載されていたもの	12事項のうち一部の事項が記載されていなかったもの（注）	12事項のうち記載されていなかった事項の数　（注）			取り扱う情報の格付に関する事項				計
				1～3事項	4～6事項	7～9事項		機密性	完全性	可用性	
本府省庁等	機関数	7	13	8	3	3	9	2	9	9	20
	システム数	86	109	79	8	22	90	21	90	90	195
地方支分部局	機関数	1	12	10	－	2	12	－	12	12	13
	システム数	2	62	60	－	2	62	－	62	62	64

（注）　整備、運用等を行っている対象システムの中に、記載されていなかった事項の数に異なる対象システムが含まれている機関があるため、「12事項のうち記載されていなかった事項の数」欄の機関数を集計しても「12事項のうち一部の事項が記載されていなかったもの」欄の機関数と一致しないものがある。

統一基準群によれば、国の行政機関等において、情報システムの情報セキュリティ水準を維持し、情報セキュリティインシデントに適切かつ迅速に対処するためには、情報セキュリティ対策に係る情報を一元的に把握することが重要であるとされている。

したがって、情報システム台帳による管理を行っていない機関や、情報システム台帳に記載することとされている12事項のうち一部の事項を記載していない機関においては、統一基準群に基づき情報システム台帳を整備する必要がある。

(ｲ) ポリシーの改定状況

統一基準群によれば、国の行政機関等はポリシーを定めなければならないこととされており、ポリシーには、統一基準群において定められている遵守事項等の規定を満たすように具体的な対策事項を規定することとされている。

3年7月に改定された統一基準群においては、国の行政機関等を標的としたサイバー攻撃や情報セキュリティインシデント等を踏まえて、より強固な情報セキュリティ対策が定められるなどしており、「政府機関等の情報セキュリティ対策のための統一基準群の改定について（通知）」（令和3年7月内閣官房内閣サイバーセキュリティセンター内閣参事官（政府機関総合対策担当）事務連絡）によれば、国の行政機関等のポリシーが、3年7月に改定された統一基準群に準拠したものとなるよう、ポリシーの改定等の対応を3年度中に行うように努めることとされていた。

本府省庁等24機関及び地方支分部局16機関のうち、ポリシーを策定しているのは、統括情報セキュリティ責任者が設置されている本府省庁等19機関(注23)であり、このうち3年7月より前からポリシーを策定していたのは18機関となっていた。

そこで、18機関におけるポリシーの改定状況を確認したところ、図表2-4のとおり、11機関は3年7月に改定された統一基準群に準拠させるためのポリシーの改定を3年度中に完了していなかった。そして、11機関のうち1機関は、ポリシーの改定を要する事項が多岐にわたり精査に時間を要しているとして、6年3月末時点においても、ポリシーの改定を完了していなかった。

（注23）　19機関以外の機関は、各府省の外局や地方支分部局等であり、本府省庁等に設置された統括情報セキュリティ責任者が策定したポリシーが適用されている。

図表2-4　統一基準群に準拠させるためのポリシーの改定状況（令和6年3月末時点）

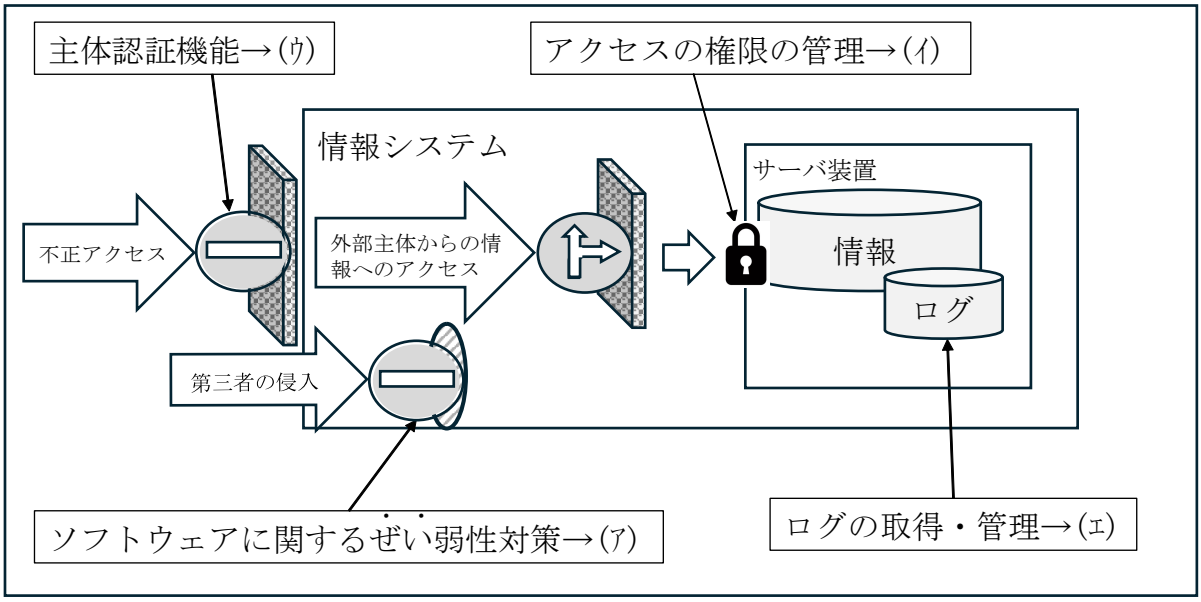
令和3年度中に改定を完了していた機関数	3年度中に改定を完了していなかった機関数	3年度末から改定の完了までに要した期間			改定が未完了	計
		1か月未満	1か月以上6か月未満	6か月以上12か月未満		
7	11	4	5	1	1	18

イ　情報システムのセキュリティ要件に係る情報セキュリティ対策の状況等

国の行政機関等の情報セキュリティインシデントに関する公表資料等によると、情報セキュリティインシデントの主な発生要因は、情報システム等のソフトウェアに関するぜい弱性の放置、一般ユーザーに管理者権限が付与されるなどのアクセス権の設定不備、パスワードの運用の不備、ログの監視の未実施、ＩＴ－ＢＣＰの未整備等となっている。

そして、これらの情報セキュリティインシデントの発生要因に対する対策として、統一基準群では、ソフトウェアに関するぜい弱性対策、アクセスの権限の管理、主体認証機能、ログの取得・管理等に係る遵守事項等が定められている（図表2-5参照）。また、政府業務継続計画等によれば、各府省庁等は、ＩＴ－ＢＣＰガイドラインに基づきＩＴ－ＢＣＰを策定することとされている。

図表2-5　情報システムのセキュリティ要件の概念図



注(1)　各枠内の右部の(ｱ)から(ｴ)までは、本報告書の記載箇所を表している。
注(2)　「「政府機関等のサイバーセキュリティ対策のための統一基準群」について」（令和4年5月内閣官房内閣サイバーセキュリティセンター作成）を基に会計検査院が作成した。

(ｱ)　ソフトウェアに関するぜい弱性対策

統一基準群では、第三者が情報システムに侵入して国の行政機関等の重要な情報を窃取し、破壊するなどの外部からの攻撃に際して、サーバ装置等で利用するソフトウェアのぜい弱性が悪用されることが想定されている。そして、統一基準群によれば、情報システムセキュリティ責任者は、ソフトウェアのぜい弱性の有無について適宜調査を行い、ソフトウェアのぜい弱性に関する情報を入手するなどした場合は、情報システムへの影響を考慮した上で、セキュリティパッチ(注24)を適用するなどのぜい弱性対策を迅速かつ適切に講ずることとされている。

そこで、対象システムにおけるソフトウェアに関するぜい弱性対策の実施状況を確認したところ、12機関の58システムについては、統一基準群に準拠したソフトウェアに関するぜい弱性対策が講じられていなかった。

ソフトウェアに関するぜい弱性が悪用された場合には、外部からの攻撃により

対象システムが有効に機能しなくなるおそれがあることから、上記の12機関においては、統一基準群に準拠したソフトウェアに関するぜい弱性対策を講ずる必要がある。

（注24） セキュリティパッチ　既に公開されているソフトウェア等において発見されたぜい弱性等に対処するために製造元等から提供されるプログラム

(ｲ) アクセスの権限の管理

統一基準群によれば、情報システム等にアクセスする者等（以下「主体」という。）の権限の管理が適切でない場合、情報システム等への不正アクセスが生ずるおそれがあるため、権限を適切に管理することが必要であるとされている。

そこで、対象システムにおけるアクセスの権限の管理状況を確認したところ、16機関の26システムについては、アクセスの権限の管理が統一基準群に準拠しておらず、適切に行われていなかった。

アクセスの権限の管理が適切でない場合には、本来権限を有しない者が対象システムや情報にアクセスし、情報の漏えいや改ざんが行われるなどして、対象システムが有効に機能しなくなるおそれがあることから、上記の16機関においては、統一基準群に準拠したアクセスの権限の管理を行う必要がある。

(ｳ) 主体認証情報の管理

統一基準群によれば、情報システム等にアクセス可能な主体を制限するためには、主体認証機能の導入が必要であるとされ、その際には、アクセス権限のある主体へのなりすましやぜい弱性を悪用した攻撃による不正アクセス行為を防止するための対策を講ずることが重要となるとされている。そして、主体認証機能を設けるに当たっては、知識による認証(注25)、所有による認証(注26)、生体による認証(注27)等の主体認証方式を決定し、導入することとされている。また、情報システムにアクセスする全ての主体に対して、主体認証情報(注28)を適切に付与し、管理するための措置を講ずることとされている。

そこで、対象システムにおける主体認証情報の管理状況を確認したところ、18機関の55システムについては、主体認証情報の管理が統一基準群に準拠しておらず、適切に行われていなかった。

主体認証情報の管理が適切でない場合には、主体になりすました者が対象シス

テムや情報に不正にアクセスし、情報の漏えいや改ざんが行われるなどして、対象システムが有効に機能しなくなるおそれがあることから、上記の18機関においては、統一基準群に準拠した主体認証情報の管理を行う必要がある。

（注25）　知識による認証　　本人のみが知り得るパスワード等の情報による認証

（注26）　所有による認証　　電子証明書を格納するＩＣカード等の本人のみが所有する機器等による認証

（注27）　生体による認証　　指紋や静脈等の本人の生体的な特徴による認証

（注28）　主体認証情報　　主体認証するために、主体が情報システムに提示する情報。代表的な主体認証情報としてパスワード等がある。

(ｴ) ログの取得・管理

統一基準群によれば、ログは、悪意のある第三者による不正侵入や不正操作等の情報セキュリティインシデントに係る事後の調査過程での問題解決、及びその予兆を検知するための重要な材料であるなどとされている。そして、情報システムの特性に応じて、ログを取得する目的を設定した上で、ログとして取得する情報項目を定めることとされており、当該情報項目の例として、ログイン及びログアウト等の事象の種類が示されている。また、取得したログの点検又は分析を定期的に実施する機能を情報システムに設けることにより、第三者による不正侵入や不正操作等の有無について点検又は分析を実施することとされている。

そこで、対象システムにおけるログの取得状況等を確認したところ、19機関の102システムについては、統一基準群に例として示されている情報項目のログ（以下「点検対象ログ」という。）が全く取得されていなかった。また、12機関の38システムについては、点検対象ログは取得されていたものの、ログの点検又は分析が実施されていなかった。

点検対象ログの取得、点検又は分析が適切に実施されていない場合には、情報セキュリティインシデントの発生が検知できずに対処が遅れるなどして、対象システムが有効に機能しなくなるおそれがあることから、上記の19機関及び12機関においては、統一基準群に準拠したログの取得・管理を行う必要がある。

(ｵ) ＩＴ－ＢＣＰの策定及び運用

ａ　ＩＴ－ＢＣＰの策定等

政府業務継続計画によれば、各府省庁等は、ＩＴ－ＢＣＰを策定することとされている。また、統一基準群によれば、統括情報セキュリティ責任者は、危

機的事象発生時に情報システムの運用を継続させる必要がある場合には、危機的事象発生時における情報セキュリティに係る対策事項を検討して定めることが重要であるとされている。そして、当該対策事項の例として、パスワードを設定した者以外の者が非常時に情報システムを使用しなければならない場合の実施手順について、情報セキュリティ関係規程に情報セキュリティ水準を確保した実施手順を整備することなどが示されている。

そこで、対象システムにおけるＩＴ－ＢＣＰの策定状況を確認したところ、本府省庁等24機関の146システム及び地方支分部局13機関の113システムの計37機関の259システムについては、ＩＴ－ＢＣＰが策定されていなかった。

また、整備、運用等を行っている対象システムのいずれかについてＩＴ－ＢＣＰが策定されていたのは本府省庁等18機関及び地方支分部局3機関の計21機関となっており、これらの機関を所管する15機関の統括情報セキュリティ責任者において、危機的事象発生時における情報セキュリティに係る対策事項を検討して定めているか確認したところ、図表2-6のとおり、10機関の統括情報セキュリティ責任者は、当該対策事項を定めていなかった。

図表2-6　危機的事象発生時における情報セキュリティに係る対策事項の策定状況（令和6年3月末時点）

ＩＴ－ＢＣＰが策定されていた機関数	左を所管する統括情報セキュリティ責任者が設置されていた機関数	危機的事象発生時における情報セキュリティに係る対策事項を定めていた機関数	危機的事象発生時における情報セキュリティに係る対策事項を定めていなかった機関数
21	15	5	10

ＩＴ－ＢＣＰを策定していない又はＩＴ－ＢＣＰは策定しているものの危機的事象発生時における情報セキュリティに係る対策事項を定めていない場合には、危機的事象発生時に対象システムの運用を継続できなくなるおそれがあることから、前記の37機関及び10機関においては、政府業務継続計画及びＩＴ－ＢＣＰガイドラインに基づきＩＴ－ＢＣＰの策定等を適切に実施する必要がある。

b　ＩＴ－ＢＣＰの運用

ＩＴ－ＢＣＰガイドラインによれば、国の行政機関等においては、ＩＴ－ＢＣＰの運用等を推進する運用継続最高責任者等の体制を整備し、事前対策等の

実効性を高めるために、教育訓練計画に基づく教育訓練を実施することとされている。

そこで、ＩＴ－ＢＣＰが策定されていた本府省庁等18機関の90システム及び地方支分部局3機関の5システム(注29)について、運用継続最高責任者等が定められているか確認したところ、本府省庁等9機関の67システム及び地方支分部局2機関の3システムについては、運用継続最高責任者等が定められていなかった。

また、図表2-7のとおり、運用継続最高責任者等が定められていた本府省庁等9機関の23システムのうち、1機関の1システムについては教育訓練計画が策定されておらず、1機関の6システムについては教育訓練計画は策定されているものの教育訓練が実施されていなかった。そして、運用継続最高責任者等が定められていた地方支分部局1機関の2システムについても教育訓練計画が策定されていなかった。

(注29)　地方支分部局の対象システム120システムのうち、ＩＴ－ＢＣＰが定められていなかったのは113システム、定められていたのは5システムであり、残りの2システムは、機関以外の組織が対象システムの主たる管理を行っているため、ＩＴ－ＢＣＰの策定状況が把握されていないものである。

図表2-7　運用継続最高責任者等の状況及び教育訓練の実施状況等（令和6年3月末時点）

機関	運用継続最高責任者等を設置		教育訓練計画を策定		教育訓練が未実施			教育訓練計画が未策定	
	機関数 注(1)	システム数	機関数 注(1)	システム数 a	機関数 注(1)	システム数 b	割合 b/a	機関数 注(1)	システム数
本府省庁等	9	23	9	22	1	6	27.2%	1	1
地方支分部局	注(2)　－	2	－	－	－	－	－	1	2

注(1)　整備、運用等を行っている対象システムの中に、教育訓練計画が策定されていたものと教育訓練計画が策定されていなかったものが含まれている機関があるため、「教育訓練計画を策定」欄と「教育訓練計画が未策定」欄の機関数を集計しても「運用継続最高責任者等を設置」欄の機関数と一致しない。
注(2)　地方支分部局1機関の2システムについては、運用継続最高責任者等が本府省庁等に設置されている。

(ｶ) 情報システムＩＤの付番等

デジタル庁は、標準ガイドライン群に基づき、政府情報システムの整備及び管理に関する事業を特定して、より適切な管理等を実施するために、各政府情報システムに情報システムＩＤを付番している。また、デジタル庁は、4年度に、各府省庁等に対して情報システムＩＤの付番状況について確認を求めて棚卸調査を実施し、情報システムＩＤが付番されていない既存の情報システムに付番するなどの整理を行っている。

デジタル庁は、5年4月に「情報システムＩＤの取得等実施要領（3.0版）」（以

下「ＩＤ取得要領」という。）を定めて、各府省庁等のＰＪＭＯがＰＭＯを通じてデジタル庁から情報システムＩＤを取得する際の手続等を示している。4年度に棚卸調査が実施されていることから、ＩＤ取得要領は、基本的に、新たに整備する情報システムに係る情報システムＩＤを取得する場合を想定した内容となっており、既存の情報システムに係る情報システムＩＤを取得する場合の手続等については明確に記載されていない。

また、標準ガイドライン群によれば、ＰＭＯは、各府省庁等内の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て、迅速な課題対応等が可能となるようにすることとされている。そして、ＰＭＯは、政府情報システムの整備等に係るプロジェクトのうち社会的重要度の高いプロジェクト等を指定して、当該プロジェクトに係る調達仕様書の作成段階において情報セキュリティ対策が適正なものとなっているか確認し、ＰＪＭＯに対して指導等を行うこととされている。

ａ　情報システムＩＤの付番

各対象システムに情報システムＩＤが付番されているかを確認したところ、本府省庁等の対象システムのうち、情報システムＩＤが付番されている情報システム（以下「ＩＤ付きシステム」という。）は23機関の194システム（本府省庁等の対象システムの82.2％）、情報システムＩＤが付番されていない情報システム（以下「ＩＤ無しシステム」という。）は13機関の42システム（同17.7％）となっていた。また、地方支分部局の対象システムのうち、ＩＤ付きシステムは13機関の25システム（地方支分部局の対象システムの20.8％）、ＩＤ無しシステムは10機関の95システム（同79.1％）となっていた。

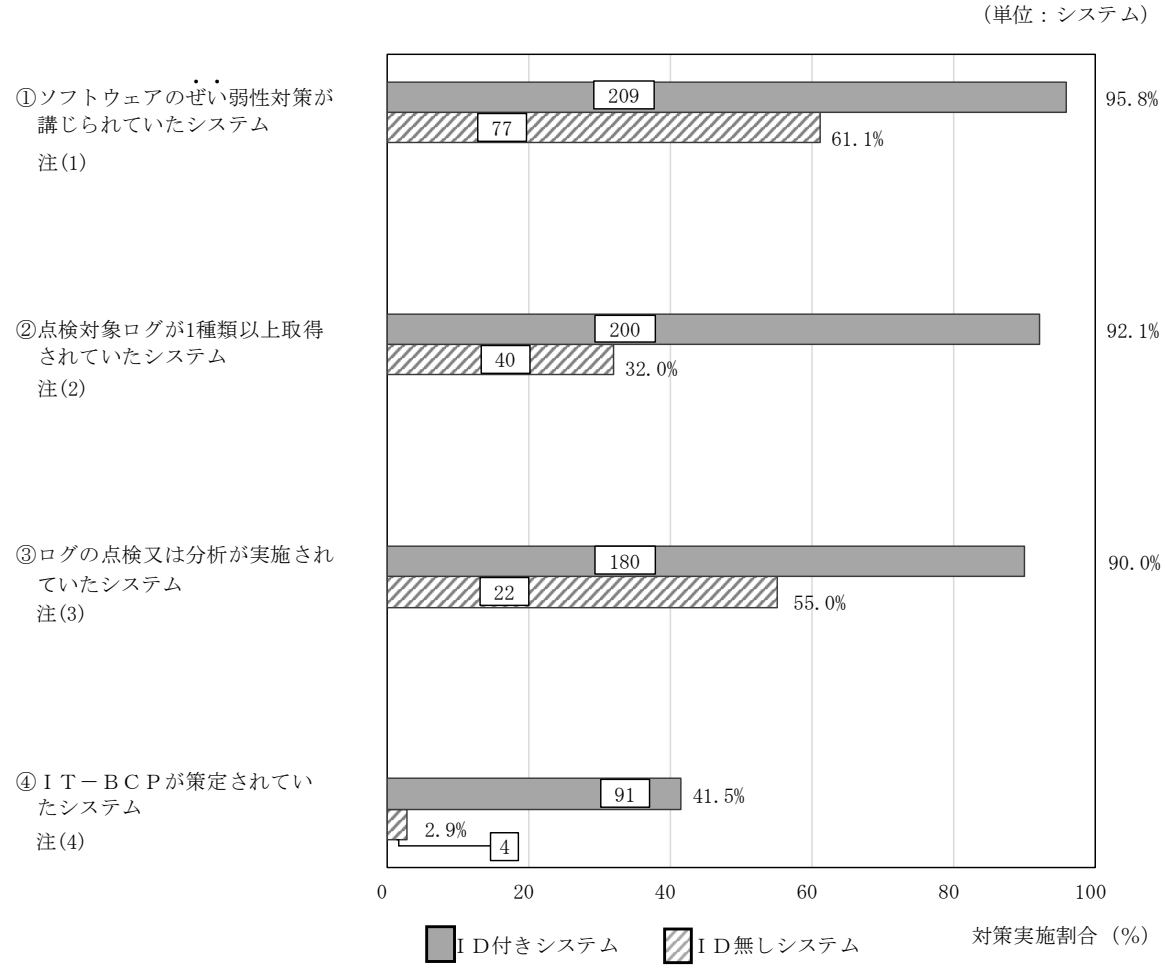
これについて、デジタル庁は、各府省庁等の情報システムが政府情報システムに該当するかどうかは、各府省庁等において一義的に判断されるものであり、また、情報システムＩＤは、基本的に各府省庁等からの申請を受けて付番するものであることから、ＩＤ無しシステムとしてどのような情報システムがあるかについては把握していないとしていた。

ｂ　情報システムＩＤの付番状況別の情報セキュリティ対策の実施状況

ＩＤ付きシステムとＩＤ無しシステムの別に、①ソフトウェアに関するぜい弱性対策、②ログの取得、③ログの点検又は分析及び④ＩＴ－ＢＣＰの策定に

係る情報セキュリティ対策の実施状況をみると、図表2-8のとおり、いずれについてもＩＤ無しシステムは、ＩＤ付きシステムよりも実施割合が低くなっていた。

図表2-8　情報システムＩＤの付番状況別の情報セキュリティ対策の実施状況



注(1)　民間事業者等が提供しているサービスを利用しているなどの12システムを除いた344システム（ＩＤ付きシステム218システム、ＩＤ無しシステム126システム）を集計の対象としている。
注(2)　民間事業者等が提供しているサービスを利用しているなどの14システムを除いた342システム（ＩＤ付きシステム217システム、ＩＤ無しシステム125システム）を集計の対象としている。
注(3)　「③ログの点検又は分析が実施されていたシステム」は、「②点検対象ログが1種類以上取得されていたシステム」の240システム（ＩＤ付きシステム200システム、ＩＤ無しシステム40システム）を集計の対象としている。
注(4)　機関以外の組織が対象システムの主たる管理を行っているため、ＩＴ－ＢＣＰの策定状況が把握されていない2システムを除いた354システム（ＩＤ付きシステム219システム、ＩＤ無しシステム135システム）を集計の対象としている。

このように、対象システムのうち本府省庁等13機関の42システム及び地方支分部局10機関の95システムの計23機関の137システムはＩＤ無しシステムとなっており、ＩＤ無しシステムは、ＩＤ付きシステムよりも情報セキュリティ対策の実施割合が低くなっていた。

一方で、対象システムは、いずれも重要な業務を実施するための情報システムであることから、情報システムＩＤを取得することにより、政府情報システムとしてデジタル庁による監理等が実施され、情報セキュリティ対策についてＰＭＯによる確認、指導等が行われることが望ましい。

したがって、ＩＤ無しシステムの整備、運用等を行っている23機関においては、必要に応じてデジタル庁と協議するなどして、情報システムＩＤの取得について検討するとともに、デジタル庁においては、ＩＤ取得要領を改定するなどして、既存の情報システムに係る情報システムＩＤを取得する場合の手続等を明確にすることについて検討することが重要である。

ウ　業務委託及び外部サービスの利用に係る情報セキュリティ対策の実施状況

(ｱ) 業務委託に係る情報セキュリティ対策の実施状況

ａ　業務の委託先における情報セキュリティ対策

国の行政機関等においては、情報システムの開発、運用等の業務を実施するに当たり、その一部を外部の業者に委託することが一般的になっている。

統一基準群によれば、国の行政機関等が、情報システム等の開発、運用等の業務を外部の業者に委託する際には、委託先において実施する情報セキュリティ対策に関する次の7事項について、調達仕様書等に定めることとされている。

①　委託先に提供する情報の委託先における目的外利用の禁止

②　委託先における情報セキュリティ対策の実施内容及び管理体制

③　委託事業の実施に当たり、委託先企業若しくはその従業員、再委託先又はその他の者によって、国の行政機関等の意図せざる変更が加えられないための管理体制（以下、この事項を「管理体制に係る事項」という。）

④　委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

⑤　情報セキュリティインシデントへの対処方法

⑥　情報セキュリティ対策その他の契約の履行状況の確認方法（以下、この事項を「確認方法に係る事項」という。）

⑦　情報セキュリティ対策の履行が不十分な場合の対処方法

このうち、管理体制に係る事項については、サプライチェーン・リスク(注30)への

対応が課題となっていることから調達仕様書等に定めることとなっているものである。また、確認方法に係る事項については、情報システムセキュリティ責任者等が、委託先における情報セキュリティ対策等の実施状況について確認する必要があることを踏まえて調達仕様書等に定めることとなっているものである。

対象システムのうち要機密情報(注31)を取り扱う対象システム(注32)について本府省庁等及び地方支分部局が3年度から5年度までに行った経費の支払に係る契約(注33)のうち、業務委託に係る契約は、本府省庁等16機関の1,138件及び地方支分部局16機関の213件となっている。そして、これらの契約において、調達仕様書等に定めることとされている7事項が定められているか確認したところ、図表2-9のとおり、本府省庁等15機関の921件（1,138件の80.9%）及び地方支分部局16機関の198件（213件の92.9%）の契約においては、7事項のうち一部の事項が定められていなかった。

(注30)　サプライチェーン・リスク　情報システム開発の委託先をはじめとした関係組織によって、不正プログラム等が委託元である政府機関の意図に反して情報システムに埋め込まれ、情報窃取が行われるなどのリスク

(注31)　要機密情報　国の行政機関における業務で取り扱う情報のうち、「行政文書の管理に関するガイドライン」（平成23年4月内閣総理大臣決定）に定める秘密文書としての取扱いを要する情報及び「行政機関の保有する情報の公開に関する法律」（平成11年法律第42号）第5条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報

(注32)　情報システム台帳において要機密情報を取り扱う対象システムとされているかどうかに基づき区分しており、情報システム台帳に記載されていない対象システムは含めていない。

(注33)　改正令による改正前の予算決算及び会計令において、契約書の作成を省略することができることとなっていた契約額が150万円を超えない契約を除く。

図表2-9　委託先において実施する情報セキュリティ対策に関する7事項の調達仕様書等における記載状況（令和3年度～5年度）

（単位：件）

年度	機関	7事項の全てが定められていた契約	7事項のうち一部の事項が定められていなかった契約		管理体制に係る事項が定められていなかった契約		確認方法に係る事項が定められていなかった契約		計
			a	割合 a/d	b	割合 b/a	c	割合 c/a	d
令和3	本府省庁等	108	386	78.1%	170	44.0%	173	44.8%	494
	地方支分部局	5	87	94.5%	68	78.1%	69	79.3%	92
4	本府省庁等	112	410	78.5%	185	45.1%	174	42.4%	522
	地方支分部局	7	88	92.6%	65	73.8%	64	72.7%	95
5	本府省庁等	101	426	80.8%	148	34.7%	148	34.7%	527
	地方支分部局	6	90	93.7%	69	76.6%	66	73.3%	96
計	本府省庁等	217〔11〕	921〔15〕	80.9%	398〔14〕	43.2%	389〔14〕	42.2%	1,138〔16〕
	地方支分部局	15〔3〕	198〔16〕	92.9%	146〔15〕	73.7%	157〔15〕	79.2%	213〔16〕

注(1)　国庫債務負担行為による複数年度契約の件数は、契約期間が含まれる全ての年度に計上しているため、各年度の件数を集計しても計欄と一致しない。
注(2)　計欄の〔 〕書きは、当該契約を締結していた機関数である。

また、確認方法に係る事項が調達仕様書等に定められていた本府省庁等15機関の749件及び地方支分部局7機関の56件の契約について、調達仕様書等に基づいて実際に確認が実施されたかどうかみたところ、図表2-10のとおり、本府省庁等14機関の233件（749件の31.1%）及び地方支分部局6機関の23件（56件の41.0%）の契約については、情報システムセキュリティ責任者等において、委託先における情報セキュリティ対策等の実施状況に係る確認が実施されていなかった。

図表2-10　委託先における情報セキュリティ対策等の実施状況に係る確認の状況（令和3年度～5年度）

（単位：件）

年度	機関	確認が実施されていた契約	確認が実施されていなかった契約		計
				割合	
			a	a/b	b
令和3	本府省庁等	212	109	33.9%	321
	地方支分部局	15	8	34.7%	23
4	本府省庁等	239	109	31.3%	348
	地方支分部局	20	11	35.4%	31
5	本府省庁等	269	110	29.0%	379
	地方支分部局	22	8	26.6%	30
計	本府省庁等	516 〔14〕	233 〔14〕	31.1%	749 〔15〕
	地方支分部局	33 〔5〕	23 〔6〕	41.0%	56 〔7〕

注(1)　国庫債務負担行為による複数年度契約の件数は、契約期間が含まれる全ての年度に計上しているため、各年度の件数を集計しても計欄と一致しない。
注(2)　計欄の〔 〕書きは、当該契約を締結していた機関数である。

b　業務の再委託先における情報セキュリティ対策

統一基準群によれば、委託先が業務の一部を再委託する場合は、①委託先において実施することとされている情報セキュリティ対策が再委託先においても実施されるよう委託先に担保させること、及び②再委託先における情報セキュリティ対策の実施状況を確認するために必要な情報を委託先が国の行政機関等に提供して、再委託について承認を受けることについて、調達仕様書等に定めることとされている（以下、これらの調達仕様書等に定める2事項を合わせて「再委託に係る事項」という。）。

業務委託に係る契約（本府省庁等16機関の1,138件及び地方支分部局16機関の213件）のうち再委託が実施されていた契約は本府省庁等16機関の551件及び地方支分部局10機関の75件となっている。そして、これらの契約において、調達仕様書等に再委託に係る事項が定められているか確認したところ、図表2-11のとおり、本府省庁等13機関の213件（551件の38.6%）及び地方支分部局10機関の62件（75件の82.6%）の契約においては、再委託に係る事項のいずれか又は両方が定められていなかった。

また、再委託に係る事項の全てが調達仕様書等に定められていた本府省庁等

13機関の338件及び地方支分部局3機関の13件の契約について、各機関が再委託を承認するに当たり、再委託先における情報セキュリティ対策の実施状況を確認するために必要な情報が実際に提供されたかを確認したところ、図表2-11のとおり、本府省庁等12機関の93件（338件の27.5%）及び地方支分部局3機関の11件（13件の84.6%）の契約においては、当該情報が提供されていなかった。

図表2-11　再委託に係る事項の調達仕様書等への記載状況等（令和3年度～5年度）

（単位：件）

年度	機関	再委託が実施されていた契約	再委託に係る事項の全てが定められていた契約	再委託先における情報セキュリティ対策の実施状況を確認するために必要な情報が提供されていなかった契約		再委託に係る事項のいずれか又は両方が定められていなかった契約		情報セキュリティ対策が再委託先においても実施されるよう委託先に担保させることを定めていなかった契約		再委託先における情報セキュリティ対策の実施状況を確認するために必要な情報を委託先が国の行政機関等に提供して、再委託について承認を受けることを定めていなかった契約	
		a	b	c	割合 c/b	d=a-b	割合 d/a	e	割合 e/d	f	割合 f/d
令和3	本府省庁等	239	133	30	22.5%	106	44.3%	30	28.3%	106	100.0%
	地方支分部局	34	7	6	85.7%	27	79.4%	15	55.5%	27	100.0%
4	本府省庁等	279	168	47	27.9%	111	39.7%	28	25.2%	111	100.0%
	地方支分部局	39	6	5	83.3%	33	84.6%	15	45.4%	33	100.0%
5	本府省庁等	300	189	51	26.9%	111	37.0%	15	13.5%	111	100.0%
	地方支分部局	43	5	5	100.0%	38	88.3%	20	52.6%	38	100.0%
計	本府省庁等	551〔16〕	338〔13〕	93〔12〕	27.5%	213〔13〕	38.6%	47〔8〕	22.0%	213〔13〕	100.0%
	地方支分部局	75〔10〕	13〔3〕	11〔3〕	84.6%	62〔10〕	82.6%	33〔8〕	53.2%	62〔10〕	100.0%

注(1)　国庫債務負担行為による複数年度契約の件数は、契約期間が含まれる全ての年度に計上しているため、各年度の件数を集計しても計欄と一致しない。
注(2)　計欄の〔 〕書きは、当該契約を締結していた機関数である。

上記について、事例を示すと次のとおりである。

＜事例1＞　再委託に係る事項の一部が調達仕様書等に定められていなかったもの

Ｃ機関は、令和4年度に、Ｃ機関の各部局が共通して利用する対象システムの更改及び運用保守に係る業務委託契約を締結している。本件契約の契約書によれば、受注者は、業務の一部を再委託する必要があるときは、あらかじめ再委託申請書を提出して、承認を受けなければならないこととされている。

また、Ｃ機関のポリシー等によれば、委託先が業務の一部を再委託する場合は、再委託先における情報セキュリティ対策の実施状況を確認するために必要な情報を委託先が発注者に提供して、再委託について承認を受けることを調達仕様書等に定めることとされている。

本件契約の調達仕様書等について確認したところ、Ｃ機関の情報システム担当者は、本件契約の調達仕様書等を作成するに当たり、本件契約と同様の内容の過去の契約の調達仕様書等を参照しており、ポリシー等に基づき再委託に係る事項の全てを調達仕様書等に定める必要があることを認識していなかった。

そのため、本件契約の調達仕様書等には、再委託先における情報セキュリティ対策の実施状況を確認するために必要な情報を委託先が発注者であるＣ機関に提供することが定められ

ていなかった。そして、C機関は、委託先からの再委託申請書の提出を受けて再委託を承認した際に、委託先から当該情報の提供を受けていなかった。
　なお、C機関は、会計検査院の検査を受けて、本件契約と同様の契約を7年度に締結する際は、ポリシー等に基づき再委託に係る事項を調達仕様書に定めている。

情報システム等の開発、運用等の業務を外部の業者に委託した際に、委託先又は再委託先において情報セキュリティ対策が適切に講じられていない場合には、第三者が委託先又は再委託先を経由して対象システムや情報に不正にアクセスし、情報の漏えい、改ざんが行われるなどして、対象システムが有効に機能しなくなるおそれがある。

したがって、委託先において実施する情報セキュリティ対策に関する事項及び再委託先に係る事項を適切に調達仕様書等に定めていない機関や、委託先における情報セキュリティ対策等の実施状況に係る確認を実施していない、又は再委託先における情報セキュリティ対策の実施状況を確認するために必要な情報の提供を受けていない機関においては、統一基準群に準拠した業務委託に係る情報セキュリティ対策を講ずる必要がある。

(ｲ) 外部サービスの利用に係る情報セキュリティ対策の実施状況

a　クラウドサービスの利用申請等

国の行政機関等においては、クラウド・バイ・デフォルト原則に基づく調達により、クラウドサービス等の外部サービスの利用が拡大している。一方、統一基準群によれば、クラウドサービス等の利用においては、情報が適正に取り扱われているかを直接確認することが一般に容易ではないなどとされており、クラウドサービス等を利用して要機密情報を取り扱う場合は、クラウドサービス等がセキュリティ要件を満たすことを確実にすることが求められるとされている。そして、情報システムセキュリティ責任者等が統括情報セキュリティ責任者等の許可権限者(注34)に利用申請を行って、クラウドサービス等がセキュリティ要件を満たすことなどを許可権限者が審査した上で利用の可否を決定することとされている。

要機密情報を取り扱う対象システムについて本府省庁等及び地方支分部局が3年度から5年度までに行った経費の支払に係る契約のうち、クラウドサービスの利用に係る契約は、本府省庁等14機関の95件及び地方支分部局5機関の12件と

なっている。そして、これらの契約に基づくクラウドサービスの利用について、許可権限者から承認を受けているか確認したところ、本府省庁等11機関の68件（95件の71.5%）及び地方支分部局4機関の10件（12件の83.3%）の契約については、許可権限者から承認を受けていなかった。

（注34）　許可権限者　　クラウドサービスの利用申請の許可権限者。原則として統括情報セキュリティ責任者であることが想定されているが、組織の特性等に応じて柔軟に定めることが可能とされている。

b　クラウドサービスのセキュリティ要件

統一基準群によれば、クラウドサービスを利用して要機密情報を取り扱う場合は、クラウドサービスのセキュリティ要件がＩＳＭＡＰ(注35)管理基準の管理策基準が求める対策と同等以上の水準（以下「管理策水準」という。）となるように調達仕様書等を定めることとされている。

そこで、要機密情報を取り扱う対象システムにおけるクラウドサービスの利用に係る契約（本府省庁等14機関の95件及び地方支分部局5機関の12件）について、クラウドサービスのセキュリティ要件が管理策水準となるように調達仕様書等に定められているか確認したところ、本府省庁等12機関の39件（95件の41.0%）及び地方支分部局3機関の5件（12件の41.6%）の契約においては定められていなかった。

そして、これらの39件及び5件の契約により利用するクラウドサービスがＩＳＭＡＰのクラウドサービスリストに登録されているか確認したところ、本府省庁等11機関の31件及び地方支分部局3機関の5件の契約については、管理策水準のセキュリティ要件を満たすクラウドサービスとして同リストに登録されているクラウドサービスを利用していたが、本府省庁等4機関の8件の契約については、同リストに登録されていないクラウドサービスを利用していた。

（注35）　ＩＳＭＡＰ管理基準　　クラウドサービス事業者がＩＳＭＡＰに係る登録申請を行う上で実施すべき情報セキュリティ管理・運用の基準であり、このうち管理策基準には、業務実施者が実施すべきアクセス管理等の情報セキュリティ対策が示されている。

クラウドサービスの利用について許可権限者から承認を受けていない場合や、クラウドサービスのセキュリティ要件が管理策水準となるように調達仕様書等を定めずに、ＩＳＭＡＰのクラウドサービスリストに登録されていないクラウドサービスを利用している場合には、セキュリティ要件を満たしていないクラウドサ

ービスにおいて情報セキュリティインシデントが発生して、対象システムが有効に機能しなくなるおそれがある。

したがって、許可権限者から承認を受けていない機関や、セキュリティ要件が管理策水準となるように調達仕様書等を定めずに、クラウドサービスリストに登録されていないクラウドサービスを利用している機関においては、統一基準群に準拠した外部サービスの利用に係る情報セキュリティ対策を講ずる必要がある。

(3) 情報セキュリティ対策に係る教育等及び監査の状況

ア　情報セキュリティ対策に関する教育等の状況

(ｱ) 各府省庁等における教育の実施状況

ポリシー及び情報セキュリティ関係規程が適切に整備されていても、その内容が職員等に認知されていなければ、適切な情報セキュリティ対策が講じられないおそれがある。

統一基準群によれば、統括情報セキュリティ責任者は、情報セキュリティ対策に関する教育について、対策推進計画(注36)に基づき、次のことを実施することとされている。

① 職員等が毎年度最低1回は教育を受けることができるように教育実施計画を策定すること

② 職員等の異動又は着任後3か月以内に教育を受けることができるように体制を整備すること

③ 職員等の役割に応じて、最新の脅威の動向、各機関の実状等を踏まえて教育すべき内容を検討し、教育のための資料を整備すること

そこで、情報セキュリティ対策に関する教育実施計画が策定されているか確認したところ、図表3-1のとおり、3年度から5年度までの各年度に、19府省庁等(注37)のうち1府省庁等においては、教育実施計画が策定されていなかった。

また、教育実施計画に基づき実施された教育の内容を確認したところ、3、4両年度に、1府省庁等においては、ポリシーの内容に関する教育が実施されていなかった。

(注36)　対策推進計画　　情報セキュリティ対策を総合的に推進するための計画

(注37)　本府省庁等24機関及び地方支分部局16機関のうち、統括情報セキュリティ責任者が設置されているのは本府省庁等19機関であり、19機関の統括情報セキュリティ責任者が19府省庁等を所管している。そして、本府省庁等の統括情報セキュリティ責任者が、統括情報セキュリティ責任者が設置さ

れていない外局や地方支分部局等を含む府省庁等全体を所管している。

図表3-1　教育実施計画の策定及び教育の実施状況（令和3年度～5年度）

年度	府省庁等数	教育実施計画が策定されていた府省庁等数		教育実施計画に基づく教育の実施状況						教育実施計画が策定されていなかった府省庁等数	
				ポリシーの内容に関する教育が実施されていた府省庁等数		業務委託に係る情報セキュリティ対策に関する教育が実施されていた府省庁等数		ポリシーの内容に関する教育が実施されていなかった府省庁等数			
	a	b	割合 b/a	c	割合 c/a	d	割合 d/a	e	割合 e/a	f	割合 f/a
令和3	17	16	94.1%	15	88.2%	11	64.7%	1	5.8%	1	5.8%
4	18	17	94.4%	16	88.8%	12	66.6%	1	5.5%	1	5.5%
5	19	18	94.7%	18	94.7%	15	78.9%	－	－	1	5.2%

注(1)　令和3年度については、関係書類が保存されていなかった1府省庁等を集計から除いている。
注(2)　令和5年4月に設置された府省庁等については、5年度のみに計上している。

また、業務委託に係る情報セキュリティ対策に関する教育が実施されていた府省庁等は、3年度11府省庁等、4年度12府省庁等、5年度15府省庁等となっていた。

一方、(2)のとおり、各機関において情報セキュリティ対策が適切に講じられていないなどの状況が見受けられており、特に、業務の委託先において実施する情報セキュリティ対策に関する7事項が調達仕様書等に適切に定められていない状況が多数の契約において見受けられた。

そこで、業務委託に係る情報セキュリティ対策に関する教育が実施されていた府省庁等の機関の契約（12機関の768件）を抽出して、調達仕様書等における記載状況を確認した。その結果、図表3-2のとおり、7事項のうち一部の事項が定められていなかった契約（11機関の633件）の割合が82.4%となるなどしており、業務委託に係る情報セキュリティ対策に関する教育が実施されていた府省庁等においても、業務委託に係る情報セキュリティ対策は必ずしも適切に講じられていない状況となっていた。

図表3-2　委託先において実施する情報セキュリティ対策に関する7事項の調達仕様書等における記載状況（業務委託に係る情報セキュリティ対策に関する教育が実施されていた府省庁等の機関の契約、令和3年度～5年度）

（単位：件）

年度	業務委託に係る契約	7事項のうち一部の事項が定められていなかった契約		管理体制に係る事項が定められていなかった契約		確認方法に係る事項が定められていなかった契約	
	a	b	割合 b/a	c	割合 c/b	d	割合 d/b
令和3	225	170	75.5%	53	31.1%	24	14.1%
4	362	291	80.3%	116	39.8%	109	37.4%
5	415	350	84.3%	106	30.2%	98	28.0%
計	768 〔12〕	633 〔11〕	82.4%	231 〔10〕	36.4%	199 〔10〕	31.4%

注(1)　国庫債務負担行為による複数年度契約の件数は、契約期間が含まれる全ての年度に計上しているため、各年度の件数を集計しても計欄と一致しない。
注(2)　計欄の〔 〕書きは、当該契約を締結していた機関数である。

教育実施計画が策定されていない場合には、統一基準群に準拠した教育が実施されないおそれがある。また、情報セキュリティ対策に関する教育を実施していても、情報セキュリティ対策が適切に講じられていない場合には、教育の内容が十分なものとなっていないおそれがある。

したがって、教育実施計画を策定していない機関においては、統一基準群に基づき教育実施計画を策定する必要がある。また、各機関においては、情報セキュリティ対策が適切に講じられるよう、ポリシーやセキュリティ関係規程の内容、情報セキュリティ対策の必要性等に関する教育を充実させるための方策について検討する必要がある。

(ｲ) ＮＩＳＣによる教育の状況

ＮＩＳＣは、ＮＩＳＣ勉強会として、国の行政機関等の情報セキュリティ対策推進体制に属する職員や情報システム担当者等を対象として、統一基準群やマネジメント監査の結果等についての講義を実施している。ＮＩＳＣによると、ＮＩＳＣ勉強会の参加者は、5年度に延べ約2,300名に上っており、講義後に実施するアンケートにより、当該講義が情報セキュリティ対策の理解に資するものとなっていることを確認しているとしていた。

一方、(2)のとおり、各機関において統一基準群に準拠した運用を行う必要があ

ることについての認識が欠けていたなどのため、情報セキュリティ対策が適切に講じられていないなどの状況が見受けられた。

したがって、ＮＩＳＣを改組して設置された国家サイバー統括室においては、これらの状況を踏まえて、対策基準策定ガイドライン等の改定に当たり、情報セキュリティ対策がより確実に講じられるよう記載内容を工夫するとともに、統一基準群の内容や情報セキュリティ対策の必要性についての理解が更に深まるように引き続き教育等の取組を進める必要がある。

(ｳ) 政府デジタル人材の配置・育成等の状況

1(3)のとおり、重点計画によれば、各府省庁等は、情報システムの適切な開発・運用やサイバーセキュリティ対策等の担い手となる人材を充実させるなどの政府デジタル人材の確保・育成等の取組を推進することとされている。また、各府省庁等が作成するデジタル人材確保・育成計画の一環として、研修の受講、デジタル人材のスキル認定等に係る具体的な目標を設定することとされている。そして、「政府デジタル人材のスキル認定の基準」によれば、スキル認定は、デジタル庁が実施する情報システム統一研修の修了等の要件を満たした者に対して行うこととされている。

また、標準ガイドラインによれば、ＰＭＯは、各府省庁等内におけるデジタル人材の育成と管理について、重点分野に人材が配分され、順調に育成されるよう、①デジタル人材確保・育成計画に係る企画立案等、②デジタル人材のスキル認定及びスキル認定を受けた者の配置状況の把握等の機能を担うこととされている。

ａ　デジタル人材のスキル認定を受けた者の配置状況の把握等

ＰＭＯが、6年3月末時点において、政府デジタル人材のスキル認定を受けた者の人数を把握しているか確認したところ、図表3-3のとおり、18府省庁等(注38)のうち16府省庁等においては、ＰＭＯがスキル認定を受けた者の人数を把握しており、当該人数は計692人となっていた。一方、2府省庁等においては、ＰＭＯがスキル認定を受けた者の人数を把握していなかった。

また、ＰＭＯがスキル認定を受けた者の配置状況を把握しているか確認したところ、人数を把握していた16府省庁等のうち11府省庁等においては、ＰＭＯがスキル認定を受けた者の配置されている部局を把握しており、対象システムの担当部局に配置されている人数は計105人、情報セキュリティ対策推進体制に

配置されている人数は計85人（11府省庁等の情報セキュリティ対策推進体制に(注39)
配置されている職員数の60.7%）となっていた。一方、5府省庁等においては、
ＰＭＯがスキル認定を受けた者の配置状況を把握していなかった。

（注38）　統括情報セキュリティ責任者と同様に、ＰＭＯが設置されているのは、本府省庁等24機関及び地方支分部局16機関のうち、本府省庁等19機関であり、19機関のＰＭＯは19府省庁等を所管している。そして、本府省庁等のＰＭＯが、ＰＭＯが設置されていない外局や地方支分部局等を含む府省庁等全体を所管している。
　また、19機関のうち政府デジタル人材のスキル認定を実施していない1機関については集計から除いている。

（注39）　スキル認定を受けた者が配置されている部局が、情報セキュリティ対策推進体制と対象システムの担当部局の両方に該当する場合があるため、85人の一部は105人と重複している。

図表3-3　スキル認定を受けた者の人数及び配置状況（令和6年3月末時点）

ＰＭＯがスキル認定を受けた者の人数を把握していた府省庁等数	スキル認定を受けた者の人数	ＰＭＯがスキル認定を受けた者の配置状況を把握					ＰＭＯがスキル認定を受けた者の配置状況を把握していなかった府省庁等数	ＰＭＯがスキル認定を受けた者の人数を把握していなかった府省庁等数
		府省庁等数	システム数	対象システムの担当部局における配置人数（注）	スキル認定を受けた者が配置されている部局で管理しているシステム数	情報セキュリティ対策推進体制における配置人数（注）		
16	692	11	104	105	40	85	5	2

（注）　スキル認定を受けた者が配置されている部局が、情報セキュリティ対策推進体制と対象システムの担当部局の両方に該当する場合には、「情報セキュリティ対策推進体制における配置人数」と「対象システムの担当部局における配置人数」の両方に計上している。

そして、ＰＭＯがスキル認定を受けた者の配置状況を把握していた11府省庁等の対象システムである104システムについて、情報システム担当部局にスキル認定を受けた者が配置されている40システムと配置されていない64システムの別に、①ソフトウェアに関するぜい弱性対策、②ログの取得、③ログの点検又は分析及び④ＩＴ－ＢＣＰの策定に係る情報セキュリティ対策の実施状況をみると、②から④までについては、スキル認定を受けた者が配置されている対象システムの方が、配置されていない対象システムよりも実施割合が高くなっ(注40)
ていた。

（注40）　①については実施割合が同じでいずれも100.0%となっていた。

b　研修の受講に係る目標の設定及び受講状況の把握

デジタル人材の確保・育成等に当たっては、デジタル人材のスキル認定等に係る目標に加えて、研修の受講に係る目標として、スキル認定の要件とされている情報システム統一研修の受講に係る目標を設定した上で、当該研修の受講の実績を把握して取組の推進に活用することが有効である。

そこで、19府省庁等において、「デジタル人材確保・育成計画」の一環として、情報システム統一研修の受講に係る目標が設定されているか確認したところ、図表3-4のとおり、5年度に当該目標が設定されていたのは15府省庁等、設定されていなかったのは4府省庁等となっていた。

また、ＰＭＯが情報システム統一研修の受講の実績を把握しているか確認したところ、図表3-4のとおり、受講の実績を把握していたのは14府省庁等、把握していなかったのは5府省庁等となっていた。

図表3-4　情報システム統一研修の受講に係る目標の設定及び受講実績の把握状況（令和3年度～5年度）

年度	項目	情報システム統一研修の受講に係る目標の設定及び受講実績の把握を実施していた府省庁等数	情報システム統一研修の受講者数　注(3)	情報システム統一研修の受講に係る目標の設定及び受講実績の把握を実施していなかった府省庁等数
令和3	目標	12	5,232	5
	実績	12	4,992	5
4	目標	14	5,258	4
	実績	14	7,352	4
5	目標	15	7,731	4
	実績	14	6,543	5

注(1)　令和3年度から5年度までの間に設置された府省庁等は、設置された年度以降（年度途中に設置された府省庁等はその翌年度以降）を集計の対象としている。
注(2)　目標及び実績の人数を概数で把握している府省庁等については、概数により集計している。
注(3)　情報システム統一研修による研修のうちスキル認定の要件とされている研修の受講者数を集計している。

イ　情報セキュリティ監査の実施状況等

統一基準群によれば、情報セキュリティ監査責任者は、監査対象、スケジュール、監査体制、監査の実施方法等を記載した監査実施計画を定めることとされている。そして、情報セキュリティ監査責任者は、情報セキュリティ監査実施者に監査実施計画に基づいて監査を実施させ、監査結果を監査報告書として最高情報セキュリティ責任者に報告することとされている（以下、監査実施計画に基づき実施する情報セキュリティ監査を「計画監査」という。）。最高情報セキュリティ責任者は、情

報セキュリティ監査責任者からの報告の内容を踏まえて、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示することとされている。そして、組織内で横断的に改善が必要な事項については、統括情報セキュリティ責任者が改善計画を策定することとされている。

(ｱ) 計画監査の実施状況等
(注41)

19府省庁等における計画監査の実施状況等を確認したところ、図表3-5のとおり、3年度は3府省庁等、4年度は2府省庁等、5年度は1府省庁等において監査実施計画が策定されていなかった。また、3年度は1府省庁等において監査実施計画は策定されていたものの、計画監査が実施されていなかった。

(注41)　統括情報セキュリティ責任者及びＰＭＯと同様に、情報セキュリティ監査責任者が設置されているのは、本府省庁等24機関及び地方支分部局16機関のうち、本府省庁等19機関であり、19機関の情報セキュリティ監査責任者は19府省庁等を所管している。そして、本府省庁等の情報セキュリティ監査責任者が、情報セキュリティ監査責任者が設置されていない外局や地方支分部局等を含む府省庁等全体を所管している。

図表3-5　計画監査の実施状況等（令和3年度～5年度）

年度	監査実施計画が策定されていた府省庁等数	計画監査			監査実施計画が策定されていなかった府省庁等数	計
		計画監査が実施されていた府省庁等数	対象システムが監査対象となっていた府省庁等数	計画監査が実施されていなかった府省庁等数		
令和3	14	13 〔127〕	7 〔17〕	1	3	17
4	16	16 〔112〕	8 〔16〕	－	2	18
5	18	18 〔303〕	6 〔13〕	－	1	19

注(1)　令和3年度については、関係書類が保存されていなかった1府省庁等を集計から除いている。
注(2)　令和5年4月に設置された府省庁等については、5年度のみに計上している。
注(3)　「計画監査が実施されていた府省庁等数」の〔 〕書きは監査の対象となった情報システム数であり、「対象システムが監査対象となっていた府省庁等数」の〔 〕書きは監査の対象となった対象システム数である。

(ｲ) 監査結果に係る情報共有の状況

19府省庁等のうち4府省庁等においては、計画監査以外に、情報システム担当部局が情報セキュリティ監査を業務委託により実施していた（以下、これらの監査を「計画外監査」という。）。

情報セキュリティ監査の結果には組織内で横断的に改善が必要な事項が含まれる場合があることから、計画外監査の結果についても、組織内で情報共有を図る

ことにより、情報セキュリティ監査責任者等が計画監査の実施方法等を検討する際の参考にするなどして組織全体の情報セキュリティ対策に活用することが有効である。

そこで、計画外監査の結果が情報セキュリティ監査責任者等に情報共有されているか確認したところ、図表3-6のとおり、4府省庁等の計画外監査に係る委託契約17件のうち14件（これらの契約により監査の対象となった対象システムは11システム）については、監査結果が情報セキュリティ監査責任者等に情報共有されていなかった。

図表3-6　計画外監査の結果に係る情報共有の状況（令和3年度～5年度）

年度	業務委託により実施されていた計画外監査			監査結果が情報セキュリティ監査責任者等に情報共有されていたもの			監査結果が情報セキュリティ監査責任者等に情報共有されていなかったもの		
	府省庁等数	契約件数	システム数	府省庁等数	契約件数	システム数	府省庁等数	契約件数	システム数
令和3	4	8	12	1	2	3	4	6	9
4	4	5	9	1	1	1	3	4	8
5	4	6	10	－	－	－	4	6	10
計	4	17	14	2	3	4	4	14	11

注(1)　国庫債務負担行為による複数年度契約は、契約期間に含まれる全ての年度の契約件数に計上しているため、各年度の件数を集計しても計欄と一致しないものがある。

注(2)　同一の対象システムについて複数の年度で計画外監査を実施している場合、各年度の対象システム数に計上しているため、各年度の対象システム数を集計しても計欄と一致しないものがある。

注(3)　監査結果が情報共有されていた年度とされていなかった年度がある対象システムがあるため、「監査結果が情報セキュリティ監査責任者等に情報共有されていたもの」と「監査結果が情報セキュリティ監査責任者等に情報共有されていなかったもの」の対象システム数の計欄を集計しても「業務委託により実施されていた計画外監査」の対象システム数の計欄と一致しない。

上記について、事例を示すと次のとおりである。

＜事例2＞　計画外監査の結果が情報セキュリティ監査責任者等に情報共有されていなかったもの

D機関は、対象システムとして、国民から申請された情報を管理することを目的とした情報システムの整備、運用等を行っている。

当該情報システムは、令和3年度から5年度までの各年度に計画監査の対象にはなっていないが、情報システム担当部局は、4年度に、当該情報システムを含めた複数の情報システムについて計画外監査を実施していた。そして、計画外監査の結果として、要機密情報を取り扱う際に用いるパスワードがポリシー等の規定を満たしていないため、ぜい弱なパスワードが使用された場合にパスワードの解読が容易となり、第三者による不正アクセスを引き起こすおそれがあると指摘されていた。

計画外監査の結果を受けて、情報システム担当部局は、当該情報システムのパスワードがポリシー等の規定を満たすように対策を講じていたものの、計画外監査の結果を情報セキュリティ監査責任者等に情報共有していなかった。

監査実施計画が策定されていない場合には、情報セキュリティ監査実施者による監査が計画的、効果的に実施されないおそれがあり、また、計画外監査の結果が情報セキュリティ監査責任者等に情報共有されない場合には、計画外監査の結果を組織全体の情報セキュリティ対策に活用することができない状況となる。

したがって、監査実施計画が策定されていなかった1府省庁等においては、統一基準群に基づき監査実施計画を策定し、当該計画に基づき監査を実施する必要がある。また、計画外監査の結果が情報セキュリティ監査責任者等に情報共有されていなかった4府省庁等においては、計画外監査の結果が情報共有されるように対応を検討する必要がある。

4　検査の状況に対する所見

(1) 検査の状況の主な内容

会計検査院は、情報システムに係る情報セキュリティ対策等の状況について、合規性、効率性、有効性等の観点から、①情報システムの整備、運用等に係る経費の支払状況及び契約の状況はどのようになっているか、②情報システムに係る情報セキュリティ対策は、統一基準群等に基づき適切に講じられているか、③情報セキュリティ対策に係る教育等及び監査は、統一基準群等に基づき適切に実施されているかなどに着眼して検査した。

なお、国家サイバー統括室は、各対象システムに係る情報セキュリティ対策等の状況に関する詳細な事実関係や、会計検査院が具体的にどのような情報システムを検査の対象としたのかなどの情報が公開された場合、特定の対象システムにおける情報セキュリティ対策等の問題点を狙い撃ちにした攻撃を誘発するなどのリスクがあるため、サイバーセキュリティを確保する観点から公開すべきではないとしている。

上記を踏まえて、これらの情報については、本報告書には記述しないこととした。

検査の状況の主な内容は次のとおりである。

ア　対象システムに係る情報セキュリティ対策の実施状況等（19～37ページ参照）

(ｱ) 対象システムに係る台帳の整備状況等

本府省庁等16機関の41システム及び地方支分部局10機関の56システムについては、情報システム台帳に記載されておらず、情報システム台帳による管理が行われていなかった。また、本府省庁等13機関の109システム及び地方支分部局12機関の62システムについては、情報システム台帳に記載することとされている12事項のうち一部の事項が記載されていなかった（20、21ページ参照）。

(ｲ) 情報システムのセキュリティ要件に係る情報セキュリティ対策の状況等

ａ　ソフトウェアに関するぜい弱性対策

12機関の58システムについては、統一基準群に準拠したソフトウェアに関するぜい弱性対策が講じられていなかった（23、24ページ参照）。

ｂ　アクセスの権限の管理

16機関の26システムについては、アクセスの権限の管理が統一基準群に準拠しておらず、適切に行われていなかった（24ページ参照）。

ｃ　主体認証情報の管理

18機関の55システムについては、主体認証情報の管理が統一基準群に準拠しておらず、適切に行われていなかった（24、25ページ参照）。

d　ログの取得・管理

19機関の102システムについては、点検対象ログが全く取得されていなかった。また、12機関の38システムについては、点検対象ログは取得されていたものの、ログの点検又は分析が実施されていなかった（25ページ参照）。

e　ＩＴ－ＢＣＰの策定及び運用

本府省庁等24機関の146システム及び地方支分部局13機関の113システムの計37機関の259システムについては、ＩＴ－ＢＣＰが策定されていなかった。

また、10機関の統括情報セキュリティ責任者は、危機的事象発生時における情報セキュリティに係る対策事項を定めていなかった（25～27ページ参照）。

f　情報システムＩＤの付番等

本府省庁等13機関の42システム及び地方支分部局10機関の95システムの計23機関の137システムはＩＤ無しシステムとなっており、ＩＤ無しシステムは、ＩＤ付きシステムよりも情報セキュリティ対策の実施割合が低くなっていた（27～30ページ参照）。

(ｳ) 業務委託及び外部サービスの利用に係る情報セキュリティ対策の実施状況

a　業務委託に係る情報セキュリティ対策の実施状況

本府省庁等15機関の921件及び地方支分部局16機関の198件の契約においては、調達仕様書等に定めることとされている7事項のうち一部の事項が定められていなかった。また、確認方法に係る事項が調達仕様書等に定められていた契約のうち、本府省庁等14機関の233件及び地方支分部局6機関の23件の契約については、情報システムセキュリティ責任者等において、委託先における情報セキュリティ対策等の実施状況に係る確認が実施されていなかった。

本府省庁等13機関の213件及び地方支分部局10機関の62件の契約においては、調達仕様書等に再委託に係る事項のいずれか又は両方が定められていなかった（30～35ページ参照）。

b　外部サービスの利用に係る情報セキュリティ対策の実施状況

本府省庁等11機関の68件及び地方支分部局4機関の10件の契約については、クラウドサービスの利用について許可権限者から承認を受けていなかった。

本府省庁等12機関の39件及び地方支分部局3機関の5件の契約においては、クラウドサービスのセキュリティ要件が管理策水準となるように調達仕様書等に定められていなかった。また、これらの契約のうち、本府省庁等4機関の8件の契約については、ＩＳＭＡＰのクラウドサービスリストに登録されていないクラウドサービスを利用していた（35～37ページ参照）。

イ　情報セキュリティ対策に係る教育等及び監査の状況（37～45ページ参照）

(ｱ) 情報セキュリティ対策に関する教育等の状況

a　各府省庁等における教育の実施状況

3年度から5年度までの各年度に、1府省庁等においては、教育実施計画が策定されていなかった。

業務委託に係る情報セキュリティ対策に関する教育が実施されていた府省庁等の機関の契約のうち、業務の委託先において実施する情報セキュリティ対策に関する7事項のうち一部の事項が定められていなかった契約の割合が82.4%となるなどしており、業務委託に係る情報セキュリティ対策に関する教育が実施されていた府省庁等においても、業務委託に係る情報セキュリティ対策は必ずしも適切に講じられていない状況となっていた（37～39ページ参照）。

b　ＮＩＳＣによる教育の状況

ＮＩＳＣによると、ＮＩＳＣ勉強会の講義後に実施するアンケートにより、当該講義が情報セキュリティ対策の理解に資するものとなっていることを確認しているとしていた。一方、各機関において統一基準群に準拠した運用を行う必要があることについての認識が欠けていたなどのため、情報セキュリティ対策が適切に講じられていないなどの状況が見受けられた（39、40ページ参照）。

(ｲ) 情報セキュリティ監査の実施状況等

3年度は3府省庁等、4年度は2府省庁等、5年度は1府省庁等において監査実施計画が策定されていなかった。

また、4府省庁等の計画外監査に係る委託契約17件のうち14件については、監査結果が情報セキュリティ監査責任者等に情報共有されていなかった（42～45ページ参照）。

(2) 所見

国の行政機関等が実施する業務においては、情報システムの利用が拡大しており、

情報システムの整備、運用等に係る経費は多額に上っている。

一方、サイバーセキュリティに対する脅威が世界規模で生じ、深刻化するなどしており、国民の安全・安心の根幹に関わる経済社会基盤を担う国の行政機関等が、サイバーセキュリティ対策を進めることにより情報セキュリティを確実に保証することが求められている。

ついては、国家サイバー統括室、デジタル庁及び各機関は、重要な業務を実施するための情報システムである対象システムに係る情報セキュリティ対策が適切に講じられ、対象システムが今後も有効に機能するよう、次の点に留意する必要がある。

ア　各機関において、統一基準群に基づき情報システム台帳を整備すること

イ　各機関において、統一基準群に準拠したソフトウェアに関するぜい弱性対策、アクセスの権限の管理、主体認証情報の管理及びログの取得・管理に係る情報セキュリティ対策を講ずること。また、政府業務継続計画及びＩＴ－ＢＣＰガイドラインに基づきＩＴ－ＢＣＰの策定等を適切に実施すること

ウ　ＩＤ無しシステムの整備、運用等を行っている各機関において、必要に応じてデジタル庁と協議するなどして、情報システムＩＤの取得について検討するとともに、デジタル庁において、ＩＤ取得要領を改定するなどして、既存の情報システムに係る情報システムＩＤを取得する場合の手続等を明確にすることについて検討すること

エ　各機関において、統一基準群に準拠した業務委託及び外部サービスの利用に係る情報セキュリティ対策を講ずること

オ　各機関において、統一基準群に基づき教育実施計画を策定するとともに、情報セキュリティ対策が適切に講じられるよう、ポリシーやセキュリティ関係規程の内容、情報セキュリティ対策の必要性等に関する教育を充実させるための方策について検討すること。また、国家サイバー統括室において、対策基準策定ガイドライン等の改定に当たり、情報セキュリティ対策がより確実に講じられるよう記載内容を工夫するとともに、統一基準群の内容や情報セキュリティ対策の必要性についての理解が更に深まるように引き続き教育等の取組を進めること

カ　各機関において、統一基準群に基づき監査実施計画を策定し、当該計画に基づき監査を実施すること。また、計画外監査の結果が情報セキュリティ監査責任者等に情報共有されるように対応を検討すること

会計検査院としては、各府省庁等の情報システムに係る情報セキュリティ対策等の状況について、引き続き注視していくこととする。

別 図 表 目 次

別図表1　マネジメント監査における指摘に係る統一基準の部別の割合等（令和5年度）

部	割合	指摘事項が多い項目
第1部　総則	―	―
第2部　情報セキュリティ対策の基本的枠組み	7.1%	（記載なし）
第3部　情報の取扱い	4.4%	（記載なし）
第4部　外部委託	14.2%	外部サービスの利用
第5部　情報システムのライフサイクル	12.0%	情報システム台帳等の整備
第6部　情報システムのセキュリティ要件	38.3%	主体認証機能、ログの取得・管理等
第7部　情報システムの構成要素	20.2%	端末・サーバ装置等
第8部　情報システムの利用	3.8%	（記載なし）

（注）　「サイバーセキュリティ2024（2023年度年次報告・2024年度年次計画）」（令和6年7月サイバーセキュリティ戦略本部決定）を基に会計検査院が作成した。

別図表2　国の行政機関等が公表している主な情報セキュリティインシデント（令和6年3月末時点）

番号	府省庁等名	公表時期	情報システムの管理組織	内容等	主な発生要因 注(2)	左に対する対応 注(2)
①	厚生労働省	令和4年11月	地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター	地方独立行政法人大阪府立病院機構大阪急性期・総合医療センターにおいて、ランサムウェア（注(1)）によるサイバー攻撃事案が発生し、電子カルテの閲覧・利用ができなくなるなどした。厚生労働省は、攻撃の侵入経路は、院外の給食調理を委託していた事業者のシステムを経由したものである可能性が高いことが判明したことを公表している。	・・ ア　機器やシステムのぜい弱性の放置 イ　一般ユーザーへの管理者権限を付与 ウ　管理者やユーザーのパス ・・ ワード運用がぜい弱（パスワード共通化等） エ　ログの監視が未実施 オ　電子カルテベンダーを始めとしたベンダーと医療機関の責任分界点（責任範囲）が、契約を含む事前の取決めがなく不明瞭 カ　情報資産の棚卸しと把握が不十分	・・ ア　保守の範囲やぜい弱性管理の役割について、機器ごとに管理者と設置者が文書により確認 イ　ユーザーは原則管理者権限のないアカウントを設定 ウ　パスワードをサーバ、端末ごとに全て個別化 エ　通信ログを確認 オ　責任分界点や役割を明確にして文書化 カ　診療情報系のネットワークに接続されているシステム等は全て情報資産として整理
②	国土交通省	5年3月	国土交通本省	河川の水位、危険性等の情報をリアルタイムで提供するシステムにおいて、簡易型河川監視カメラの画像の一部に不具合が確認されたため、国土交通省はこれらについて配信を停止した。同省は、当該カメラの通信記録等の調査を行ったところ、不正アクセスの疑いがある痕跡が確認されたことを公表している。	仕様書に記載した以下のセキュリティ対策の未実施 ・管理者パスワードの複雑化 ・使用しない通信ポート（扉）の閉塞化	・パスワードを再設定 ・使用しない通信ポートを閉塞化
③	国土交通省	5年7月	名古屋港運協会	国土交通省は、名古屋港の全てのコンテナターミナルにおけるコンテナの積卸し作業、搬入・搬出等を一元的に管理する名古屋港統一ターミナルシステムで発生した情報セキュリティインシデントにより、約3日間、同ターミナルからのコンテナの搬入・搬出が停止し、物流に大きな影響を与えたことを公表している。	ア　システム障害発生時の対応手順が事前に未整備。サイバー攻撃も対象としたシステム障害発生時のＢＣＰが未整備 ・・ イ　機器やシステムのぜい弱性への対応が未対応	ア　システム障害発生時の対応手順を整備するとともにサイバー攻撃も対象としたシステム障害発生時のＢＣＰを整備 イ　ぜい弱性対策に必要となる情報の収集、ぜい弱性対策の状況の定期確認等

注(1)　「ランサムウェア」は、感染するとパソコン等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラムのことである。

注(2)　「主な発生要因」欄及び「左に対する対応」欄は、それぞれの報告書等に基づいて記載している。
①「調査報告書」（令和5年3月地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター情報セキュリティインシデント調査委員会）
②「配信を停止している簡易型河川監視カメラの再開について」（令和5年3月国土交通省水管理・国土保全局）及び会計実地検査提出資料
③「名古屋港のコンテナターミナルにおけるシステム障害を踏まえ緊急に実施すべき対応策及び情報セキュリティ対策等の推進のための制度的措置について」（令和6年1月コンテナターミナルにおける情報セキュリティ対策等検討委員会）

別図表3　情報セキュリティ対策や情報システムの運用の継続性の状況に関する主な検査報告掲記事項等

検査報告等	府省等	件名等	内容
平成26年度決算検査報告	8府省庁	インターネット上からの通信が可能なサーバ上で利用していたサポート期間が終了しているソフトウェアの更新等を実施するとともに、ポリシー等を改定することなどによりサポート期間が終了しているソフトウェアを利用しないよう改善させたもの	宮内庁、総務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省及び環境省において、インターネット上からの通信が可能なサーバ上でサポート期間が終了しているソフトウェアを利用していたこと、サポート期間の終了を管理者が把握するまでに長期間を要していたことなどから、本院の指摘に基づき、インターネット上からの通信が可能なサーバ上で利用していた検査対象ソフトウェアの更新等を実施するとともに、サポート期間が終了しているソフトウェアを原則として利用しないことについて、ポリシー等に明記するなどの処置を講じたもの
会計検査院法第30条の2の規定に基づく報告（平成28年12月報告）	厚生労働省 日本年金機構	年金個人情報に関する情報セキュリティ対策の実施状況及び年金個人情報の流出が日本年金機構の業務に及ぼした影響等について	平成27年5月に日本年金機構が運用する情報システムの共有フォルダに保存されていた約125万件の年金個人情報がインターネットを通じて不正に外部に流出する事案が発生したことや、同事案の発生を受けて、厚生労働省及び同機構は、国民年金保険料の納付実績を向上させるための業務の一部を一定期間行わないこととするなどしたことから、同機構の業務に様々な影響が生ずるところとなったことなどを踏まえて、同機構の年金個人情報に関する情報セキュリティ対策等の状況、同事案の発生が同機構の業務に及ぼした影響等を検査し、その状況を取りまとめて報告したもの
会計検査院法第30条の2の規定に基づく報告（平成30年4月報告）	12府省庁	各府省庁の災害関連情報システムに係る整備、運用等の状況について	各府省庁は、それぞれの所掌事務等について災害に関する情報の収集、伝達等に使用するための情報システムを整備し、内閣府は、各府省庁が当該情報システムにより収集した災害関連情報を集約し、共有するなどのための総合防災情報システムを整備していることなどを踏まえて、災害関連情報システムの整備、運用等の状況を検査し、その状況を取りまとめて報告したもの
平成29年度決算検査報告及び平成30年度決算検査報告	厚生労働省	データ入力等の請負等業務における監督、検収等について	データ入力業務等の請負等業務において、承認の手続をとらずに中華人民共和国等に所在する業者に業務の一部を下請けさせており、契約の適正な履行及び機密保持の観点から適切ではない事態が見受けられたことなどから、厚生労働大臣に対して、30年10月に、会計検査院法第34条の規定により是正改善の処置を求め、及び同法第36条の規定により改善の処置を要求したもの（平成29年度決算検査報告に掲記） （その後の処置状況） 厚生労働省において、毎年度、検査職員等に対して会計法令や検査・監督実務の要点等に関する研修を実施することとするなどし、会計法令の遵守を周知徹底するなどの処置が講じられていた（平成30年度決算検査報告に掲記）。

検査報告等	府省等	件名等	内容
平成30年度決算検査報告及び令和元年度決算検査報告	総務省	情報通信技術利活用事業費補助金による事業の実施状況について	情報通信技術利活用事業費補助金による事業において、クラウドを活用した導入システムの運用について、情報セキュリティ対策が適切に講じられていないなどの事態が見受けられたことから、総務大臣に対して、令和元年10月に、会計検査院法第36条の規定により改善の処置を要求したもの（平成30年度決算検査報告に掲記） （その後の処置状況） 総務省において、情報セキュリティ対策が適切に講じられていない地方公共団体である事業主体に対して、クラウドを活用した導入システムの運用について、法の趣旨に沿って、地方公共団体が自ら定める情報セキュリティポリシー等に基づいて適切な情報セキュリティ対策を講じさせるなどの処置が講じられていた（令和元年度決算検査報告に掲記）。
会計検査院法第30条の2の規定に基づく報告（令和2年1月報告）	総務省	国による地方公共団体の情報セキュリティ対策の強化について	地方公共団体等が実施する事務において、個人番号を利用する事務及び情報連携が行われることになり、地方公共団体の情報セキュリティ対策の強化が公的機関全体にとって重要な課題となっていることなどを踏まえて、国による地方公共団体の情報セキュリティ対策の強化について、実施状況等を検査し、その状況を取りまとめて報告したもの
会計検査院法第30条の3の規定に基づく報告（令和3年5月報告）	13府省等	政府情報システムに関する会計検査の結果について	参議院から、国会法第105条の規定に基づき、各府省がサービス・業務を実施するために用いる情報システムである政府情報システムに関する①政府情報システムの整備及び運用に係る予算の執行状況、②各府省等が締結する契約の競争性、経済性の状況、③政府情報システムの利用状況及び効果の発現状況、④政府情報システム全体の効率化及びコスト削減に向けた取組状況について会計検査を行いその結果を報告することを求める要請を受けたことから、上記の各事項について検査を実施してその結果を報告したもの
令和4年度決算検査報告	日本年金機構	日本年金機構情報セキュリティポリシー等に基づいて実施すべき情報セキュリティ対策を事業担当部署に対して周知徹底することなどにより、情報システムの調達、保守等業務の外部委託等において適切な情報セキュリティ対策が講じられるよう改善させたもの	日本年金機構において、電話による相談に使用するためのコールセンター機器群について、日本年金機構情報セキュリティポリシーに基づく適切な情報セキュリティ対策が講じられておらず、相談者の年金個人情報を含む録音データが漏えいするなどのリスクが回避されているとは認められない状況となっていたことから、本院の指摘に基づき、コールセンター機器群についてセキュリティ要件の設定等を行うなどするとともに、日本年金機構情報セキュリティポリシー等に基づき、事前に情報管理対策室の確認を受けることなどを事業担当部署に対して周知徹底するなどの処置を講じたもの

別図表4　競争契約の応札者数別の契約件数及び契約額（令和3年度～5年度）

（単位：件、百万円）

年度	区分	応札者数		計
		1者	2者以上	
令和3	契約件数	290	96	386
	割合	75.1%	24.8%	100.0%
	契約額	196,461	61,134	257,595
	割合	76.2%	23.7%	100.0%
4	契約件数	264	96	360
	割合	73.3%	26.6%	100.0%
	契約額	140,131	26,706	166,838
	割合	83.9%	16.0%	100.0%
5	契約件数	208	93	301
	割合	69.1%	30.8%	100.0%
	契約額	150,251	49,397	199,649
	割合	75.2%	24.7%	100.0%
計	契約件数	762	285	1,047
	割合	72.7%	27.2%	100.0%
	契約額	486,844	137,238	624,083
	割合	78.0%	21.9%	100.0%

別図表5　情報システム台帳に記載する12事項

統一基準群（抜粋）
情報システム台帳の整備 統括情報セキュリティ責任者は、以下の内容を含む台帳を整備すること。 a）情報システム名 b）管理課室 c）当該情報システムセキュリティ責任者の氏名及び連絡先 d）システム構成 e）接続する機関等外通信回線の種別 f）取り扱う情報の格付及び取扱制限に関する事項　（注） g）当該情報システムの設計・開発、運用・保守に関する事項 また、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備すること。 a）情報処理サービス名 b）契約事業者 c）契約期間 d）情報処理サービスの概要 e）ドメイン名 f）取り扱う情報の格付及び取扱制限に関する事項　（注）

（注）　これらの事項は合わせて1事項として取り扱っている。

参考　用語集

ＣＳＩＲＴ　(Computer Security Incident Response Team)

組織内において発生した情報セキュリティインシデントに対処するために、当該組織内に設置された体制

ＩＳＭＡＰ管理基準

クラウドサービス事業者がＩＳＭＡＰに係る登録申請を行う上で実施すべき情報セキュリティ管理・運用の基準であり、このうち管理策基準には、業務実施者が実施すべきアクセス管理等の情報セキュリティ対策が示されている。

運用等経費

情報システムの運用、保守等に要する経常的な経費

オンプレミス

アプリケーションごとに個別の動作環境（サーバ等）を準備して自ら運用する形態

可用性

情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性のこと

完全性

情報が破壊、改ざん又は消去されていない特性のこと

危機的事象

不正アクセス等の運用妨害、地震等の自然災害、火災等の人的災害等の様々な事象

機密性

情報に関して、アクセスを認められた者だけがこれにアクセスできる特性のこと

許可権限者

クラウドサービスの利用申請の許可権限者。原則として統括情報セキュリティ責任者であることが想定されているが、組織の特性等に応じて柔軟に定めることが可能とされている。

クラウド

システムの整備、運用等の効率化を図るために、一元管理されたコンピュータ資源をネットワーク経由で利用する形態

サイバーセキュリティ

電子的方式等により記録される情報の漏えい、滅失又は毀損の防止等の安全管理のために必要な措置並びに情報システム等の安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること

サプライチェーン・リスク

情報システム開発の委託先をはじめとした関係組織によって、不正プログラム等が委託元である政府機関の意図に反して情報システムに埋め込まれ、情報窃取が行われるなどのリスク

主体認証

主体（情報システム等にアクセスする者等）が、正当であるか否かを検証すること

主体認証情報

主体認証するために、主体が情報システムに提示する情報。代表的な主体認証情報としてパスワード等がある。

情報システム

ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するもの

情報セキュリティインシデント

望まない又は予期しない情報セキュリティ事象であって、事業運営を危うくする又は情報セキュリティの確保に脅威を及ぼす可能性のある事象

情報の格付

統一基準群によれば、機密性、完全性及び可用性の三つの観点に区分して、観点ごとに二つ又は三つの区分に分類することとされている。

所有による認証

電子証明書を格納するＩＣカード等の本人のみが所有する機器等による認証

生体による認証

指紋や静脈等の本人の生体的な特徴による認証

整備経費

情報システムの整備（新規開発、機能改修・追加、更改及びこれらに付随する環境の整備）に要する一時的な経費

政府情報システム

各府省庁等がサービス・業務を実施するために用いる情報システム

セキュリティパッチ

既に公開されているソフトウェア等において発見されたぜい弱性等に対処するために製造元等から提供されるプログラム

対策推進計画

情報セキュリティ対策を総合的に推進するための計画

知識による認証

本人のみが知り得るパスワード等の情報による認証

要機密情報

国の行政機関における業務で取り扱う情報のうち、「行政文書の管理に関するガイドライン」（平成23年4月内閣総理大臣決定）に定める秘密文書としての取扱いを要する情報及び「行政機関の保有する情報の公開に関する法律」（平成11年法律第42号）第5条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報

ログ

システムの動作履歴、利用者のアクセス履歴、通信履歴その他運用管理等に必要な情報を記録したデータ