## 第4　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<br>(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<br>(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)<br>(2) 362億1604万円(令和3年度～5年度) |
| 報告を行った年月日 | 令和7年9月12日 |

### 1　検査の状況の主な内容

本院は、各府省庁等の情報システム(注1)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、「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)、「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)、「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)、「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、これらを合わせて「統一基準群」という。)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、サイバー安全保障分野の政策を一元的に総合調整している国家サイバー統括室(令和7年6月30日以前は内閣サイバーセキュリティセンター(以下「NISC」という。))は、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(注2)(以下「対象システム」という。)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、本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(注3)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、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。

(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

(注2)　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。

（注３） 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



### ⑴　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

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。

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

㋐　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。

㋑　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。

㋒　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(注４)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。

（注４） 主体認証情報　　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

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(注５)（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。

（注５） 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

㋔　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、「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。）に基づき策定することとなっている情報システム運用継続計画（以下「IT－BCP」という。）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(注６)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。

（注６） 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

(カ)　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。)となっており、ID無しシステムは、情報システムIDが付番されている情報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。

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

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、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のいずれか又は両方が定められていなかった。

(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

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(注7)の利用について許可権限者(注8)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政府情報システム(注9)のためのセキュリティ評価制度(以下「ISMAP」という。)管理基準(注10)の管理策基準が求める対策と同等以上の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。

(注7)　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

(注8)　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。

(注9)　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

(注10)　政府情報システムのためのセキュリティ評価制度管理基準　　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。

### ⑵　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

⑺　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。

⑻　NISCによる教育の状況

NISCによると、NISC勉強会(注11)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。

(注11)　NISC勉強会　　国の行政機関等の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の結果等について講義を実施するもの

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府省庁等において、監査実施計画に基づき実施する情報セキュリティ監査以外に情報システム担当部局が業務委託により実施していた情報セキュリティ監査(以下「計画外監査」という。)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。

## 2　検査の状況に対する所見

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（首都直下地震対策）」（平成 26 年 3 月閣議決定）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、「情報システム ID の取得等実施要領（3.0 版）」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、情報セキュリティ対策の基本的な方針、情報セキュリティ対策の基準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

本院としては、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。