４　法令等遵守の一層の推進

勧　　告	説明図表番号
平成 20 年人事院勧告（平成 20 年８月 11 日）は、「年金問題にみられる行政の「破綻」、幹部公務員の不祥事、不適切な公費支出など、公務及び公務員の在り方にかかわる問題が相次いで生じている。このため、国民の公務員への不信や批判はこれまでになく高まってきている。不祥事等が発生した場合には、その事実関係を十分把握・分析した上で適切な懲戒処分を行うなど厳正に対処し、併せて具体的な再発防止策を講じていくことが当然に求められる。」としている。 国家公務員が法令等を遵守することは、当然のことであるが、職員による不祥事等が続発し、国民の信頼を大きく損なうような事態が生じており、各府省は、不祥事に対する再発防止策を講ずるとともに、不祥事が起こりにくい態勢づくりに積極的に取り組むことが求められている。 今回、各府省における、法令等遵守の推進状況について調査した結果、次のような状況がみられた。 不祥事が起こりにくい態勢とするためには、法令等遵守について、現状を的確に把握し、その結果を分析・評価した上で、必要な改善・見直しを行うことが重要である。 その中にあって、行政機関の保有する個人情報の管理及び政府機関の情報セキュリティ対策については、次のとおり、検証・評価や改善・見直しの仕組みが整備されている。	
①　行政機関の保有する個人情報の管理については、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならないとされ、監査責任者が保有個人情報の管理の状況について監査を行うことや、保護管理者が自ら管理責任を有する保有個人情報の記録媒体、処理経路、保管方法等について点検を行うことが定められるとともに、保有個人情報の適切な管理のための措置について、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直しの措置を講ずるとされている。 また、行政機関の保有する個人情報の保護に関する法律の規定に基づき、同法の施行の状況について調査を行い、その結果を公表している。	表４－① 表１－⑴－④ （再掲）
②　政府機関の情報セキュリティ対策については、各府省庁は、政府機関全体として高いレベルで水準のそろった情報セキュリティを確保するため、情報セキュリティ対策の実施状況を自ら定期的に検査し、必要に応じて、対策の改善を行うとされ、内閣官房情報セキュリティセンターは、各府省庁の対策の実施状況を統一基準に基づき、必要な範囲で検査し、評価するとされている。 しかしながら、今回調査対象とした法令等には、行政機関の保有する個人情報の管理及び政府機関の情報セキュリティ対策で示されるような各府省において検	表４－②

証・評価や改善・見直しを行う仕組みはない。また、項目２、項目３のとおり、職員に対する周知・広報や研修の教育活動が必ずしも継続的、定期的に実施されておらず低調となっている。 　各府省は、会計監査制度を整備し、一部府省は監察制度を整備しており、不祥事が発生した場合、事後に検証・評価や改善・見直しが行われ再発防止策が講じられている。しかし、今回調査した法令等遵守を推進するための各種の制度や仕組みの中には、個々の職員への法令等遵守意識の浸透状況の把握や教育活動等においてこれらが的確に機能しているのかどうかについての検証・評価が、必ずしも十分に行われておらず、また、それらの制度や仕組みが連携して有効に機能しているかどうかの検証・評価は行われていない状況がみられる。 　したがって、各府省は、法令等遵守を一層推進し、不祥事を予防する観点から、法令等遵守に係る取組についての定期的な検証・評価を行い、その結果を公表するとともに、必要な見直しを行うという取組を一層推進していく必要がある。	

表４－①　行政機関の保有する個人情報の適切な管理のための措置

○　行政機関の保有する個人情報の適切な管理のための措置に関する指針について（通知）
（平成 16 年９月 14 日付け総管情第 84 号、各府省等官房長等あて総務省行政管理局長）＜抜粋＞

（別紙）　行政機関の保有する個人情報の適切な管理のための措置に関する指針

第２　管理体制

（監査責任者）

４　各行政機関に、監査責任者を一人置くこととし、内部監査等を担当する部局の長等をもって充てる。

監査責任者は、保有個人情報の管理の状況について監査する任に当たる。

第 10　監査及び点検の実施

（監査）

１　監査責任者は、保有個人情報の管理の状況について、定期に又は随時に監査（外部監査を含む。）を行い、その結果を総括保護管理者に報告する。

（点検）

２　保護管理者は、自ら管理責任を有する保有個人情報の記録媒体、処理経路、保管方法等について、定期に又は随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告する。

（評価及び見直し）

３　保有個人情報の適切な管理のための措置については、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等の措置を講ずる。

（注）下線は当省が付した。

表４－②　政府機関の情報セキュリティ対策

○　政府機関の情報セキュリティ対策の強化に関する基本方針
（平成 17 年９月 15 日情報セキュリティ政策会議決定）＜抜粋＞

２　対策強化のための基本方針

１の基本認識を踏まえ、政府の情報セキュリティ政策の一環として、各府省庁は以下に示す統一的・横断的な情報セキュリティ対策を推進することにより、政府機関全体として高いレベルで水準のそろった情報セキュリティを確保し、もって国民が信頼できる電子政府の実現及び継続的かつ安定的な行政機能の維持に努めることとする。

（１）政府機関統一基準の策定

各府省庁は、情報セキュリティ対策の整合化・共通化を促進することとする。情報セキュリティ政策会議（以下「政策会議」という。）は、このために必要な政府機関統一基準について定め、以後、技術や環境の変化を踏まえ、毎年その見直しを行うものとする。

（２）各府省庁での情報セキュリティポリシー等の見直し

各府省庁は、自らの組織の情報セキュリティ対策について責任を持って取り組むことを原則としたうえで、政府機関統一基準を踏まえ、現行の情報セキュリティポリシー及び情報システム関係実施手順等について必要な見直しを行うことによって、政府機関全体として整合性のある情報セキュリティ対策を促進する。

（３）各府省庁での自己点検等

各府省庁は、情報セキュリティ対策の実施状況を自ら定期的に検査し、必要に応じて、対策の改善を行う。

（４）政府全体でのＰＤＣＡサイクルの確立

内閣官房情報セキュリティセンター（以下「センター」という。）は、各府省庁の対策の実施状況を、政府統一基準に基づき、必要な範囲で検査し、評価する。これをもとに、政策会議は各府省庁の対策の改善を勧告し、政府機関統一基準等の改善に結びつけることで、政府全体としてのＰＤＣＡサイクル（Plan・Do・Check・Act サイクル）を確立する。

（５）情報セキュリティ確保に有効な制度等の活用の促進

各府省庁は、安全な情報システムの構築を推進するため、客観的に評価された暗号・製品等の導入、外部監査の実施、外部委託先の情報セキュリティ管理体制の確認等情報セキュリティ確保のために必要な措置を講ずる。また、センターは、各府省庁におけるこれらの取組みを促進する。

（注）下線は当省が付した。