（参考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に関する指針
新旧対照表

（下線部は改正箇所）

改正後	現　行
第１　（略）	第１　（略）
第２　管理体制 １　（略） （保護管理者） ２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。 保護管理者は、各課室等における保有個人情報の適切な管理を確保する任に当たる。保有個人情報を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、その任に当たる（注）。 （注）例えば、第６、第７、第９－２、第10－２、第10－３その他保有個人情報を情報システムで取り扱う場合、保護管理者は、情報システムの管理者と連携して、それぞれの措置を講ずる。 ３～５　（略）	第２　管理体制 １　（略） （保護管理者） ２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。 保護管理者は、各課室等における保有個人情報を適切に管理する任に当たる。 ３～５　（略）
第３　教育研修 １　総括保護管理者は、保有個人情報の取扱いに従事する職員（派遣労働者（注）を含む。以下同じ。）に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。 （注）保有個人情報の取扱いに従事する派遣労働者についての労働者派遣契約は、保有個人情報の適切な取扱いを行うことに配慮されたものとする必要がある。 ２　（略） ３　総括保護管理者は、保護管理者及び保護担当者に対し、課室等の現場における保有個人情報の適切な管理のための教育研修を実施する。 ４　（略）	第３　教育研修 １　総括保護管理者は、保有個人情報の取扱いに従事する職員に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。 ２　（略） （新設） ３　保護管理者は、当該課室等の職員に対し、保有個人情報の適切な管理のために、総括保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。
（削除）	４　１～３の措置を講ずる場合には、保有個人情報の取扱いに従事する派遣労働者についても、職員と同様の措置を講ずる。
第４　（略）	第４　（略）
第５　個人情報の取扱い （アクセス制限） １　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。 ２・３　（略） （複製等の制限） ４　職員が業務上の目的で保有個人情報を取り扱う場合であっても、保護管理者は、次に	第５　個人情報の取扱い （アクセス制限） １　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する者をその利用目的を達成するために必要最小限の職員に限る。 ２・３　（略） （複製等の制限） ４　職員は、業務上の目的で保有個人情報を取り扱う場合であっても、次に掲げる行為につ

掲げる行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を限定し、職員は、保護管理者の指示に従い行う。 (1)　保有個人情報の複製 (2)　保有個人情報の送信 (3)　保有個人情報が記録されている媒体の外部への送付又は持出し (4)　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為	いては、保護管理者の指示に従い行う。 (1)　保有個人情報の複製 (2)　保有個人情報の送信 (3)　保有個人情報が記録されている媒体の外部への送付又は持出し (4)　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為
５～８　（略）	５～８　（略）
第６　情報システムにおける安全の確保等 （アクセス制御） １　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（16を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる（注）。 （注）アクセス制御の措置内容は、第５－１により設定した必要最小限のアクセス権限を具体化するものである必要がある。	第６　情報システムにおける安全の確保等 （アクセス制御） １　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（10を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる。
２　保護管理者は、１の措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。	２　保護管理者は、１の措置を講ずる場合には、パスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。
３・４　（略）	３・４　（略）
（アクセス状況の監視） ５　保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずる。	（アクセス状況の監視） ５　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報への不適切なアクセスの監視のため、一定数以上の保有個人情報がダウンロードされた場合に警告表示がなされる機能の設定、当該機能の定期的確認等の必要な措置を講ずる。
６・７　（略）	６・７　（略）
（不正プログラムによる漏えい等の防止） ８　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。	（不正プログラムによる漏えい等の防止） ８　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、不正プログラムの感染防止等に必要な措置を講ずる。
（情報システムにおける保有個人情報の処理） ９　職員は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。	（新設）
（暗号化） 10　保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置	（暗号化） ９　保護管理者は、保有個人情報の秘匿性等その内容に応じて、その暗号化のために必要な

を講ずる。 職員（注）は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。 （注）職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。	措置を講ずる。
11　（略）	（記録機能を有する機器・媒体の接続制限） 17　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい、滅失又は毀損の防止のため、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。
12　（略）	（端末の限定） 13　保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。
13　（略）	（端末の盗難防止等） 14　保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。
14　（略）	15　職員は、保護管理者が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。
15　（略）	（第三者の閲覧防止） 16　職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。
16　（略）	（入力情報の照合等） 10　職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。
17　（略）	（バックアップ） 11　保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。
18　（略）	（情報システム設計書等の管理） 12　保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。
第７　（略）	第７　（略）
第８　保有個人情報の提供及び業務の委託等 １　（略） ２　保護管理者は、法第８条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずる。	第８　保有個人情報の提供及び業務の委託等 １　（略） ２　保護管理者は、法第８条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い措置状況を確認し、その結果を記録するとともに、改善要求等の措置を講ずる。

３～７　（略）	３～７　（略）
第９　安全確保上の問題への対応 （事案の報告及び再発防止措置） １　保有個人情報の漏えい等安全確保の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告する（注）。 （注）職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。	第９　安全確保上の問題への対応 （事案の報告及び再発防止措置） １　保有個人情報の漏えい等安全確保の上で問題となる事案が発生した場合に、その事実を知った職員は、速やかに当該保有個人情報を管理する保護管理者に報告する。
２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のＬＡＮケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。	２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずる。
３～５　（略） （公表等） ６　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応（注）等の措置を講ずる。 公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに総務省（行政管理局）に情報提供を行う。 （注）漏えい等が生じた保有個人情報に係る本人への連絡等の対応	３～５　（略） （公表等） ６　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る本人への対応等の措置を講ずる。
第 10　監査及び点検の実施 （監査） １　監査責任者は、保有個人情報の適切な管理を検証するため、第２から第９に規定する措置の状況を含む当該行政機関における保有個人情報の管理の状況について、定期に及び必要に応じ随時に監査（外部監査を含む。以下同じ。）（注）を行い、その結果を総括保護管理者に報告する。 （注）保有個人情報の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。	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、各課室等におけ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、定期に及び必要に応じ随時に点検を行い、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。	（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　総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、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。	（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、総括保護管理者、保護管理者等は、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。
第 11　独立行政法人等に対する指導等 各行政機関は、「個人情報の保護に関する基本方針」（平成 16 年４月２日閣議決定）４に基づき、所管する独立行政法人等に対して、その業務運営における自主性に配慮しつ	（新設）

つ、個人情報の保護に関し必要な指導、助言を行う。	

独立行政法人等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
新旧対照表

（下線部は改正箇所）

改正後	現　行
第１　（略）	第１　（略）
第２　管理体制 １　（略） （保護管理者） ２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。 保護管理者は、各課室等における保有個人情報の適切な管理を確保する任に当たる。保有個人情報を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携して、その任に当たる（注）。 （注）例えば、第６、第７、第９－２、第10－２、第10－３その他保有個人情報を情報システムで取り扱う場合、保護管理者は、情報システムの管理者と連携して、それぞれの措置を講ずる。 ３～５　（略）	第２　管理体制 １　（略） （保護管理者） ２　保有個人情報を取り扱う各課室等に、保護管理者を一人置くこととし、当該課室等の長又はこれに代わる者をもって充てる。 保護管理者は、各課室等における保有個人情報を適切に管理する任に当たる。 ３～５　（略）
第３　教育研修 １　総括保護管理者は、保有個人情報の取扱いに従事する職員（派遣労働者（注）を含む。以下同じ。）に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。 （注）保有個人情報の取扱いに従事する派遣労働者についての労働者派遣契約は、保有個人情報の適切な取扱いを行うことに配慮されたものとする必要がある。 ２　（略） ３　総括保護管理者は、保護管理者及び保護担当者に対し、課室等の現場における保有個人情報の適切な管理のための教育研修を実施する。 ４　（略） （削除）	第３　教育研修 １　総括保護管理者は、保有個人情報の取扱いに従事する職員に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。 ２　（略） （新設） ３　保護管理者は、当該課室等の職員に対し、保有個人情報の適切な管理のために、総括保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。 ４　１～３の措置を講ずる場合には、保有個人情報の取扱いに従事する派遣労働者についても、職員と同様の措置を講ずる。
第４　（略）	第４　（略）
第５　個人情報の取扱い （アクセス制限） １　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。 ２・３　（略） （複製等の制限） ４　職員が業務上の目的で保有個人情報を取	第５　個人情報の取扱い （アクセス制限） １　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する者をその利用目的を達成するために必要最小限の職員に限る。 ２・３　（略） （複製等の制限） ４　職員は、業務上の目的で保有個人情報を取

り扱う場合であっても、保護管理者は、次に掲げる行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を限定し、職員は、保護管理者の指示に従い行う。 (1)　保有個人情報の複製 (2)　保有個人情報の送信 (3)　保有個人情報が記録されている媒体の外部への送付又は持出し (4)　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為	り扱う場合であっても、次に掲げる行為については、保護管理者の指示に従い行う。 (1)　保有個人情報の複製 (2)　保有個人情報の送信 (3)　保有個人情報が記録されている媒体の外部への送付又は持出し (4)　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為
５～８　（略）	５～８　（略）
第６　情報システムにおける安全の確保等 （アクセス制御） １　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（16を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる（注）。 （注）アクセス制御の措置内容は、第５－１により設定した必要最小限のアクセス権限を具体化するものである必要がある。	第６　情報システムにおける安全の確保等 （アクセス制御） １　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第６（10を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる。
２　保護管理者は、１の措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。	２　保護管理者は、１の措置を講ずる場合には、パスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。
３・４　（略）	３・４　（略）
（アクセス状況の監視） ５　保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずる。	（アクセス状況の監視） ５　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報への不適切なアクセスの監視のため、一定数以上の保有個人情報がダウンロードされた場合に警告表示がなされる機能の設定、当該機能の定期的確認等の必要な措置を講ずる。
６・７　（略）	６・７　（略）
（不正プログラムによる漏えい等の防止） ８　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。	（不正プログラムによる漏えい等の防止） ８　保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、不正プログラムの感染防止等に必要な措置を講ずる。
（情報システムにおける保有個人情報の処理） ９　職員は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。	（新設）
（暗号化） 10　保護管理者は、保有個人情報の秘匿性等そ	（暗号化） ９　保護管理者は、保有個人情報の秘匿性等そ

の内容に応じて、暗号化のために必要な措置を講ずる。 職員（注）は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。 （注）職員が行う暗号化には、適切なパスワードの選択、その漏えい防止の措置等が含まれる。	の内容に応じて、その暗号化のために必要な措置を講ずる。
11　（略）	（記録機能を有する機器・媒体の接続制限） 17　保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい、滅失又は毀損の防止のため、スマートフォン、ＵＳＢメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。
12　（略）	（端末の限定） 13　保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。
13　（略）	（端末の盗難防止等） 14　保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。
14　（略）	15　職員は、保護管理者が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。
15　（略）	（第三者の閲覧防止） 16　職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。
16　（略）	（入力情報の照合等） 10　職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。
17　（略）	（バックアップ） 11　保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。
18　（略）	（情報システム設計書等の管理） 12　保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。
第７　（略）	第７　（略）
第８　保有個人情報の提供及び業務の委託等 １　（略） ２　保護管理者は、法第９条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善	第８　保有個人情報の提供及び業務の委託等 １　（略） ２　保護管理者は、法第９条第２項第３号及び第４号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い措置状況を確認し、その結果を記録するとともに、改善

要求等の措置を講ずる。 ３～７　（略）	要求等の措置を講ずる。 ３～７　（略）
第９　安全確保上の問題への対応 （事案の報告及び再発防止措置） １　保有個人情報の漏えい等安全確保の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告する（注）。 （注）職員は、当該事案の発生（事案発生のおそれを含む。）を認識した場合、時間を要する事実確認を行う前にまず保護管理者に報告する。	第９　安全確保上の問題への対応 （事案の報告及び再発防止措置） １　保有個人情報の漏えい等安全確保の上で問題となる事案が発生した場合に、その事実を知った職員は、速やかに当該保有個人情報を管理する保護管理者に報告する。
２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のＬＡＮケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。	２　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずる。
３・４　（略）	３・４　（略）
５　総括保護管理者は、事案の内容等に応じて、事案の内容、経緯、被害状況等について、当該独立行政法人等を所管する行政機関に対し、速やかに情報提供を行う。	（新設）
６　（略） （公表等） ７　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応（注）等の措置を講ずる。 公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに総務省（行政管理局）に情報提供を行う。 （注）漏えい等が生じた保有個人情報に係る本人への連絡等の対応	５　（略） （公表等） ６　事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る本人への対応等の措置を講ずる。
第 10　監査及び点検の実施 （監査） １　監査責任者は、保有個人情報の適切な管理を検証するため、第２から第９に規定する措置の状況を含む当該独立行政法人等における保有個人情報の管理の状況について、定期に及び必要に応じ随時に監査（外部監査を含む。以下同じ。）（注）を行い、その結果を総括保護管理者に報告する。 （注）保有個人情報の秘匿性等その内容及びその量に応じて、実地監査を含めた重点的な監査として行うものとする。	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、各課室等におけ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、定期に及び必要に応じ随時に点検を行い、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。	（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　総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、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。	（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、総括保護管理者、保護管理者等は、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。

第 11　行政機関との連携 　各独立行政法人等は、「個人情報の保護に関する基本方針」（平成 16 年４月２日閣議決定）４を踏まえ、当該独立行政法人等を所管する行政機関と緊密に連携して、その保有する個人情報の適切な管理を行う。	（新設）