資料１－３

特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（平成２６年特定個人情報保護委員会告示第６号）の一部改正案の新旧対照表

〇平成２６年特定個人情報保護委員会告示第６号（特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編））

（傍線部分は改正部分）

改正案	現行
（別添）特定個人情報に関する安全管理措置 （行政機関等・地方公共団体等編） 【目次】 1　（略） 2　講ずべき安全管理措置の内容 Ａ、Ｂ　（略） Ｃ　組織的安全管理措置 ａ～ｃ　（略） ｄ　情報漏えい等事案に対応する体制等の整備 ｅ　（略） Ｄ　人的安全管理措置 ａ　（略） ｂ　事務取扱担当者等の教育 ｃ　法令・内部規程違反等に対する厳正な対処 Ｅ　（略） Ｆ　技術的安全管理措置 ａ、ｂ　（略） ｃ　不正アクセス等による被害の防止等	（別添）特定個人情報に関する安全管理措置 （行政機関等・地方公共団体等編） 【目次】 1　（略） 2　講ずべき安全管理措置の内容 Ａ、Ｂ　（略） Ｃ　組織的安全管理措置 ａ～ｃ　（略） ｄ　情報漏えい等事案に対応する体制の整備 ｅ　（略） Ｄ　人的安全管理措置 ａ　（略） ｂ　事務取扱担当者の教育 （新設） Ｅ　（略） Ｆ　技術的安全管理措置 ａ、ｂ　（略） ｃ　不正アクセス等の防止

改正案	現行
ｄ　（略）	**ｄ　（略）**
1　（略）	**1　（略）**
2　講ずべき安全管理措置の内容	**2　講ずべき安全管理措置の内容**
Ａ、Ｂ　（略）	**Ａ、Ｂ　（略）**
Ｃ　組織的安全管理措置	**Ｃ　組織的安全管理措置**
ａ～ｃ　（略）	**ａ～ｃ　（略）**
ｄ　情報漏えい等事案に対応する体制等の整備 情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制及び手順等を整備する。 情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。 **≪手法の例示≫** ＊　情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制及び手順等を整備することが考えられる。 ・　情報漏えい等の事案が発覚した際の報告・連絡等 ・　事実関係の調査及び原因の究明 ・　影響を受ける可能性のある本人への連絡 ・　委員会及び主務大臣等への報告	**ｄ　情報漏えい等事案に対応する体制の整備** 情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する。 情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。 **≪手法の例示≫** ＊　情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制を整備することが考えられる。 ・　事実関係の調査及び原因の究明 ・　影響を受ける可能性のある本人への連絡 ・　委員会及び主務大臣等への報告

改正案	現行
・　再発防止策の検討及び決定 ・　事実関係及び再発防止策等の公表 ＊　不正アクセス、ウイルス感染の事案に加え、標的型攻撃等の被害を受けた場合の対応について、関係者において定期的に確認又は訓練等を実施する。	・　再発防止策の検討及び決定 ・　事実関係及び再発防止策等の公表
e　取扱状況の把握及び安全管理措置の見直し 監査責任者（地方公共団体等においては相当する者）は、特定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点検又は監査（外部監査を含む。）を行い、その結果を総括責任者（地方公共団体等においては相当する者。以下同じ。）に報告する。総括責任者は、点検又は監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。	**e　取扱状況の把握及び安全管理措置の見直し** 監査責任者（地方公共団体等においては相当する者）は、特定個人情報の管理の状況について、定期に又は随時に点検又は監査（外部監査を含む。）を行い、その結果を総括責任者（地方公共団体等においては相当する者。以下同じ。）に報告する。総括責任者は、点検又は監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。
D　人的安全管理措置	**D　人的安全管理措置**
a　（略）	**a　（略）**
b　事務取扱担当者等の教育 総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等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。 また、特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、特定個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必	**b　事務取扱担当者の教育** 総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等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。また、特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、特定個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。

改正案	現行
要な教育研修を行う。 総括責任者は、保護責任者に対し、課室等における特定個人情報等の適正な管理のために必要な教育研修を行う。 総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適切な管理のために、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。 **ｃ　法令・内部規程違反等に対する厳正な対処** 法令又は内部規程等に違反した職員に対し、法令又は内部規程等に基づき厳正に対処する。 **Ｅ　（略）** **Ｆ　技術的安全管理措置** **ａ、ｂ　（略）** **ｃ　不正アクセス等による被害の防止等** 情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組み等を導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。 個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏まえたシステム構築や運用体制整備を行う。	総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適切な管理のために、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。 **（新設）** **Ｅ　（略）** **Ｆ　技術的安全管理措置** **ａ、ｂ　（略）** **ｃ　不正アクセス等の防止** 情報システムを外部等からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。また、個人番号利用事務の実施に当たり接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置を遵守する。

≪手法の例示≫ ＊　特定個人情報等を取り扱う情報システムと外部ネットワーク（又はその他の情報システム）との接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 ＊　情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。 ＊　導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。 ＊　機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ＊　定期に及び必要に応じ随時にログ等の分析を行い、不正アクセス等を検知する。 ＊　不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用する。 ＊　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講ずる。	≪手法の例示≫ ＊　情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。 ＊　情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。 ＊　導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。 ＊　機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ＊　ログ等の分析を定期的に行い、不正アクセス等を検知する。 ＊　情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講ずることが考えられる。
d　情報漏えい等の防止 特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。 特定個人情報ファイルを機器又は電子媒体等に保存する必要が	**d　情報漏えい等の防止** 特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。

改正案	現行
ある場合、原則として、暗号化又はパスワードにより秘匿する。 **≪手法の例示≫** ＊　通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。 ＊　暗号化又はパスワードによる秘匿に当たっては、不正に入手した者が容易に復元できないように、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮する。	**≪手法の例示≫** ＊　通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。 ＊　情報システム内に保存されている特定個人情報等の情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等が考えられる。