【資料2－3】ガイドライン改訂に向けた論点整理表

資料2－3

「ガイドライン改定に向けた論点整理表」(本書)について

■「ガイドライン改定に向けた論点整理表」の位置づけ
・本整理表は、各種基準・文献、構成員からの意見などから抽出した改定ポイントと改定方針を整理したドキュメントです。
・研究会では、本整理表の中から特に議論が必要な論点を抽出し討議して頂きます。
（資料2－1「情報セキュリティポリシーガイドライン」改定のための論点についてを利用します）
・資料2－1に論点として出ていないものについても、本方針に沿って改定作業を進めてまいりますので、方針にご意見をいただけます場合は10月15日（水）までに事務局までご意見いただきますようお願い致します。

■改定内容の種類
・ガイドラインの改定内容には大きく3つに分類されると想定しております。
・ガイドライン改定による自治体職員の方々へのインパクトという観点で分類しています。

改定区分	改定内容
明確化	・既存のガイドラインにおいて曖昧になっていた点を明確にする改定 ・自治体にとっては迅速な判断ができるようになる可能性が高い
管理強化	・既存のガイドライン上の管理策を強化する改定 ・自治体にとっては負荷・コスト面の負担を強いる可能性が高い
推奨	・改定ポイント候補として設定するものの、改定による自治体へのマイナスインパクトが懸念されることから実施は推奨とする （例： インパクトを踏まえたうえで、対応可能な自治体は実施することが望ましい）

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
1	「0 ポリシーガイドライン全体」	現行の情報セキュリティポリシーガイドラインには、「権限・責任者一覧」が添付されているが、利用方法が分かりにくいため	現行の情報セキュリティポリシー運用上の課題	構成員からのご意見	ポリシーガイドラインの対象者が誰かを明確化させ、ポリシーガイドラインの記述内容を明確化する必要がある	明確化	2	・ポリシーガイドラインの想定する読者や読者のスキルレベルを「1.1.本ガイドラインの目的」に記載する	「権限・責任者一覧」等をうまく活用しながら、ポリシーガイドライン上の対象者を明確化する観点で、検討を行う
2	「0 ポリシーガイドライン全体」	現行の情報セキュリティポリシーガイドラインには、セキュリティレベルの考え方の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	構成員からのご意見	ポリシーガイドラインがどのレベルの団体向けなのかが分かり辛い	明確化	2	・ポリシーガイドラインの対象とする団体について「1.1.本ガイドラインの目的(P2)」に追記する ・「市」を想定した記述であることを追記する ※備考：小規模団体における組織体制の確立に関する注意事項については、「1.6.2.組織体制の確立(P8)」にて現状でも記述されている。	ポリシーガイドライン上に段階的にセキュリティ対応力を向上させていく観点で、検討を行う
3	「1.6 策定及び導入」	現行の情報セキュリティポリシーガイドラインに、環境の変化があった後の対応方法が明確に記述されていないため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	新しい技術（スマートフォン、クラウド等）の導入や新たな脅威等の環境の変化があった後、リスク分析、ポリシー見直し等の一連の見直し等につながっていない	明確化	10、13	・現行のポリシーガイドライン「1.6.4.リスク分析の実施(P10)」に、「情報セキュリティに関する環境の変化や監査・点検の結果、情報資産や情報資産に対する…」を追記する ・現行のポリシーガイドライン「1.8.2.情報セキュリティポリシーの見直し(P13)」の図表8に、「新たな情報機器(スマートデバイス)やサービス(クラウド)の利用」を追記する	環境の変化やポリシーガイドラインの改定があった場合に一連の対応が実施できている団体の進め方、体制、事例なども参考にしながら、情報セキュリティ対策の見直しを徹底する観点で検討する。 特に、新しい情報技術に対する情報セキュリティ対応指針や対応事例などの情報提供も検討する。
4	「1.6.4 リスク分析の実施」	リスク分析の実施に関しては、「地方公共団体における情報資産のリスク分析・評価に関する手引き（平成21年3月）」が参照されているが、実施方法に関して見直す必要があるため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	主要な情報資産について調査及びリスク分析は、（地方自治情報管理概要の平成25年度によると）都道府県では約60%、市区町村は約30%の実施率にとどまっており、実施できない理由に難しさと時間がかかる点をあげている	明確化	9～10	・現行のポリシーガイドライン「1.6.4.リスク分析の実施(P10)」に、簡易リスク分析方法等についての追記修正を行う	簡易リスク分析等を含めた、現場で実施しやすいリスク分析の方法を検討する
5	「1.7 運用」	現行の情報セキュリティポリシーガイドラインに、環境の変化があった後の対応方法が明確に記述されていないため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	新しい技術（スマートフォン、クラウド等）の導入や新たな脅威等の環境の変化があった後、リスク分析、ポリシー見直し等の一連の見直し等につながっていない	明確化	10、13	・現行のポリシーガイドライン「1.6.4.リスク分析の実施(P10)」に、「情報セキュリティに関する環境の変化や監査・点検の結果、情報資産や情報資産に対する…」を追記する ・現行のポリシーガイドライン「1.8.2.情報セキュリティポリシーの見直し(P13)」の図表8に、「新たな情報機器(スマートデバイス)やサービス(クラウド)の利用」を追記する	環境の変化やポリシーガイドラインの改定があった場合に一連の対応が実施できている団体の進め方、体制、事例なども参考にしながら、情報セキュリティ対策の見直しを徹底する観点で検討する。 特に、新しい情報技術に対する情報セキュリティ対応指針や対応事例などの情報提供も検討する。
6	「1.8 評価・見直し」	現行の情報セキュリティポリシーガイドラインに、環境の変化があった後の対応方法が明確に記述されていないため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	新しい技術（スマートフォン、クラウド等）の導入や新たな脅威等の環境の変化があった後、リスク分析、ポリシー見直し等の一連の見直し等につながっていない	明確化	10、13	・現行のポリシーガイドライン「1.6.4.リスク分析の実施(P10)」に、「情報セキュリティに関する環境の変化や監査・点検の結果、情報資産や情報資産に対する…」を追記する ・現行のポリシーガイドライン「1.8.2.情報セキュリティポリシーの見直し(P13)」の図表8に、「新たな情報機器(スマートデバイス)やサービス(クラウド)の利用」を追記する	環境の変化やポリシーガイドラインの改定があった場合に一連の対応が実施できている団体の進め方、体制、事例なども参考にしながら、情報セキュリティ対策の見直しを徹底する観点で検討する。 特に、新しい情報技術に対する情報セキュリティ対応指針や対応事例などの情報提供も検討する。
7	「1.8 評価・見直し」	現行の情報セキュリティポリシーガイドラインには、監査結果や点検結果を元にした見直し（リスク分析、セキュリティポリシー、実施手順等）の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	定期的な監査・点検は、約40%の団体が実施しており、定着しつつあるものの、監査結果や点検結果を元にした見直しが実施されていない課題がある	明確化	13	・現行ポリシーガイドライン「1.8.1.監査・自己点検(P13)」に、監査を実施する上での参考資料として「地方公共団体における情報セキュリティ監査に関するガイドライン」を追記する	監査や点検実施後の一連の対応が実施できている団体の進め方、体制、事例なども参考にしながら、情報セキュリティ対策の見直しを徹底する観点で、検討を行う
8	「3.2 組織体制」	現行の情報セキュリティポリシーガイドラインには、情報セキュリティに関する人材育成方法に関する観点が弱いため	現行の情報セキュリティポリシー運用上の課題	構成員からのご意見	情報セキュリティに関する人材育成方法として、相互監査を実施したり、地域の中心となる団体の人材が周辺団体の人材教育を行う方法がある。また、CISO補佐官の民間人活用のような方法もある	明確化	27	・現行ポリシーガイドライン(P26-27)では、CIO、及びCIO補佐官について記載されているため、この部分にCISO補佐官の記述を追記する ・解説（2）(P27)に「注」を追加し、CISO補佐官の記述を追記	情報セキュリティに関する人財育成や民間活用に関する観点から、見直し検討を行う

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
9	「3.2 組織体制」	現行の情報セキュリティポリシーガイドラインには、大規模な障害・事故等に関する連絡網や体制に観点が弱いため	現行の情報セキュリティポリシー運用上の課題	NISC統一基準（平成26年度版） 2.2.4	緊急連絡網には当該システムに係る責任者及び管理者のほか、大規模な障害・事故等に備えて最高情報セキュリティ責任者も含める必要がある	明確化	24	ポリシーガイドライン(P24)に大規模インシデント発生時の緊急連絡体制について追記する	大規模な障害・事故等に備えての体制、連絡網の観点で見直し検討する
10	「3.2 組織体制」	現行の情報セキュリティポリシーガイドラインには、現場でのセキュリティ事件・事故対応に関する体制の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	構成員からのご意見	各団体の現場でセキュリティ事件や事故等の対応ができる仕組み（CSIRT: ComputerSecurityIncidentResponseTeam）が必要である	管理強化	26、 28-29	・現行ポリシーガイドライン「3.2.組織体制(P26)」に、「CSIRT」の記述を「推奨事項」として追記する ・現行ポリシーガイドライン「3.2.組織体制」の「解説(P28-29)」にCSIRTの組織体制例として図表を追記する	各団体の現場でセキュリティ事件や事故等の対応ができる仕組み（CSIRT: ComputerSecurityIncidentResponseTeam）作りの観点で見直し検討する
11	「3.3 情報資産の分類と管理方法」	リスク分析の実施に関しては、「地方公共団体における情報資産のリスク分析・評価に関する手引き（平成21年3月）」が参照されているが、実施方法に関して見直す必要があるため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	主要な情報資産について調査及びリスク分析は、（地方自治情報管理概要の平成25年度によると）都道府県では約60%、市区町村は約30%の実施率にとどまっており、実施できない理由に難しさと時間がかかる点をあげている	明確化	9～10	・現行のポリシーガイドライン「1.6.4.リスク分析の実施(P10)」に、簡易リスク分析方法等についての追記修正を行う	簡易リスク分析等を含めた、現場で実施しやすいリスク分析の方法を検討する
12	「3.4.3 通信回線及び通信回線装置の管理」	現行の情報セキュリティポリシーガイドラインには、通信回線の可用性の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	NISC統一基準（平成26年度版） 7.3.1	（通信回線の可用性の強化） 要安定情報を取り扱う情報システムについては、通信回線装置の運用状態を復元するために必要な処置を講ずること （障害・事故等によりサービスを提供できない状態が発生した場合に、サービスの可用性を担保することを目的としている）	管理強化	42	現行のポリシーガイドライン(P42)に重要情報を扱うシステムに接続された回線の継続的運用を可能とするための措置について追記する	要安定情報を取り扱う情報システムについての、通信回線装置の運用状態を復元するための観点を検討する
13	「3.4.4 職員等のパソコン等の管理」	モバイル機器（スマートフォン等）のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	スマートフォン・クラウドセキュリティ研究会最終報告会（総務省平成24年6月29日）	スマートフォン端末の紛失・盗難等に対する情報の漏えい等の対策をパソコンと同様に行う事が望ましい。	明確化	10、44 47-48	・現行ポリシーガイドライン「3.1.対象範囲(P23)」の図表10の情報システムに「スマートデバイス」の記述を追記 ・現行ポリシーガイドライン「3.4.4.職員等のパソコン等の管理(P44)(解説)」に、スマートデバイスにおけるパスワード等による端末ロック、紛失時に備えたりモードワイプ機能の利用【推奨事項】について追記 ・同ガイドライン「3.5.1.職員等の遵守事項(P47-48)（解説）」にスマートデバイスについても文言を追記	スマートフォンのセキュリティ対策の考え方をパソコンと同様に追加検討する。
14	「3.5.1 職員等の順守事項」	支給品以外の端末利用に関するセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 8.2	「支給以外の端末の利用」 端末に情報を保存させず、支給以外の端末を業務利用することを可能とする。仕組みとして、シンクライアントやリモートデスクトップの技術の活用が有効	管理強化	45,47	現行のポリシーガイドライン(P46)に、支給以外の端末を使用する場合の、盗難、紛失、不正プログラム対策について追記する	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、支給品以外の端末の利用時のセキュリティ対策の観点を追加検討する
15	「3.5.1 職員等の順守事項」	ソーシャルメディアサービスによる情報発信に関するセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 4.1.3	（ソーシャルメディアサービスによる情報発信） (a)アカウントによる情報発信が本物か、成りすまし対策を講ずること (b)パスワード等の生体認証情報を適切に管理するなどの不正アクセス対策を実施すること 情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含めなければならない。	管理強化	46,48	現行のポリシーガイドライン(P46)にソーシャルメディアサービスによる情報発信についての基準を追記する	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、ソーシャルメディアサービスによる情報発信時の対策等を検討する
16	「3.5.1 職員等の順守事項」	USBメモリ等の外部記憶媒体等のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 8.1.1	USBメモリ等の外部電磁記録媒体を用いた利用基準をきめること (a)支給の媒体を利用する（私物や出所不明の媒体を使用しない） (b)紛失・盗難リスク防止 (c)セキュアな外部媒体の利用（暗号化）	明確化	45	現行のポリシーガイドライン(P45)にUSBメモリ等の利用基準に関して追記する	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、USBメモリ等の外部電磁記録媒体を用いた利用基準の観点を追加検討する
17	「3.5.1 職員等の順守事項」	モバイル機器（スマートフォン等）のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A6.2.1	モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用しなければならない。	明確化	10、44 47-48	・現行ポリシーガイドライン「3.1.対象範囲(P23)」の図表10の情報システムに「スマートデバイス」の記述を追記 ・現行ポリシーガイドライン「3.4.4.職員等のパソコン等の管理(P44)(解説)」に、スマートデバイスにおけるパスワード等による端末ロック、紛失時に備えたりモードワイプ機能の利用【推奨事項】について追記 ・同ガイドライン「3.5.1.職員等の遵守事項(P47-48)（解説）」にスマートデバイスについても文言を追記	モバイル機器のセキュリティ対策の考え方を追加検討する。

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
18	「3.5.1 職員等の順守事項」	無線LAN利用時のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	一般利用者が安心して無線LANを利用するために（総務省平成24年11月2日）	無線LAN情報セキュリティ3つの約束 （約束1）無線LANを利用するときは大事な情報はSSLでやりとり （約束2）無線LANを公共で使用するときは、ファイル共有機能を解除 （約束3）自分でアクセスポイントを設置する場合には、適切な暗号化方式を設定	明確化	58、62	・現行ポリシーガイドライン「3.6.1.コンピュータ及びネットワーク管理(P58)(例文)、(P62)（解説）」に職員等が無線LAN利用する時の注意事項について追記 ・参考文献として「一般利用者が安心して無線LANを利用するために」も追記する	無線LAN利用時のセキュリティ対策の考え方を追加検討する。
19	「3.5.1 職員等の順守事項」	モバイル機器（スマートフォン等）のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	クラウドサービス提供における情報セキュリティ対策ガイド(平成26年4月総務省) 6.2.1	モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用することが望ましい。	明確化	10、44 47-48	・現行ポリシーガイドライン「3.1.対象範囲(P23)」の図表10の情報システムに「スマートデバイス」の記述を追記 ・現行ポリシーガイドライン「3.4.4.職員等のパソコン等の管理(P44)(解説)」に、スマートデバイスにおけるパスワード等による端末ロック、紛失時に備えたりモードワイプ機能の利用【推奨事項】について追記 ・同ガイドライン「3.5.1.職員等の遵守事項(P47-48)（解説）」にスマートデバイスについても文言を追記	モバイル機器のセキュリティ対策の考え方を追加検討する。
20	「3.5.1 職員等の順守事項」	個人利用機器(パソコン、モバイル機器、記憶媒体など)の業務利用や持込みの制限に対する記述が弱いため	今後検討すべき情報セキュリティポリシーの課題	組織における内部不正防止ガイドライン（情報処理推進機構） （11）	個人利用機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用することが望ましい。	明確化	48	・現行ガイドラインの「3.5.1.職員等の遵守事項(P48)(解説)」に個人の情報機器及び記録媒体の業務利用及び持込み制限について記述を追記	個人利用機器に対するセキュリティ対策の考えを追加検討する
21	「3.5.1 職員等の順守事項」	在宅勤務（テレワーク）における情報セキュリティ管理に関する観点が弱いため	－	運用上の課題	在宅勤務（テレワーク）時のリスクや脅威を把握し、適切な対策を実施する必要がある	明確化	48	・現行ガイドラインの「3.5.1.職員等の遵守事項(P48)(解説)」に在宅勤務（テレワーク）における対策を追記	在宅勤務（テレワーク）に対するセキュリティ対策を明確化する
22	「3.5.2 研修・訓練」	現行の情報セキュリティポリシーガイドラインには、情報セキュリティに関する人材育成方法に関する観点が弱いため	現行の情報セキュリティポリシー運用上の課題	構成員からのご意見	情報セキュリティに関する人材育成方法として、相互監査を実施したり、地域の中心となる団体の人材が周辺団体の人材教育を行う方法がある。また、CISO補佐官の民間人活用のような方法もある	明確化	51	・現行ポリシーガイドライン「3.5.2.件数・訓練(P51)（解説）」に、外部の専門家をCISO補佐官として招聘し、内部教育にも活用したり、近隣の同規模の自治体間で相互監査・点検などを行って人材育成に寄与させることを追記	情報セキュリティに関する人財育成や民間活用に関する観点から、見直し検討を行う
23	「3.5.3 事故・欠陥等の報告」	現行の情報セキュリティポリシーガイドラインには、情報セキュリティに関する障害・事故等の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	NISC統一基準（平成26年度版） 2.2.4	（情報セキュリティに関する障害・事故等の対応） 障害・事故等の発生に備えた事前準備、発生時における報告と応急処置、原因調査と再発防止策についての順守事項を定める	明確化	52	現行のポリシーガイドライン(P52)に、インシデント対応の体制整備や準備事項、原因調査について追記する	障害・事故等の発生に備えた事前準備、発生時における報告と応急処置、原因調査と再発防止策についての観点で見直し検討する
24	「3.6.1 コンピュータ及びネットワークの管理」	無線LAN利用時のセキュリティ対策の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	一般利用者が安心して無線LANを利用するために（総務省平成24年11月2日）	無線LAN情報セキュリティ3つの約束 （約束1）無線LANを利用するときは大事な情報はSSLでやりとり （約束2）無線LANを公共で使用するときは、ファイル共有機能を解除 （約束3）自分でアクセスポイントを設置する場合には、適切な暗号化方式を設定	明確化	58、62	・現行ポリシーガイドライン「3.6.1.コンピュータ及びネットワーク管理(P58)(例文)、(P62)（解説）」に職員等が無線LAN利用する時の注意事項について追記 ・参考文献として「一般利用者が安心して無線LANを利用するために」も追記する	無線LAN利用時のセキュリティ対策の考え方を追加検討する。
25	「3.6.1 コンピュータ及びネットワークの管理」	無線LAN利用時のセキュリティ対策の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	企業等が安心して無線LANを導入・運用するために（総務省平成25年1月30日）	無線LANにおいて、組織のLAN管理者がとるべき情報セキュリティ対策及び無線LANの導入・運用の各段階において実施すべき事項。	明確化	58、62	・現行ポリシーガイドライン「3.6.1.コンピュータ及びネットワーク管理(P58)(例文)、(P62)（解説）」に統括情報セキュリティ責任者として無線LAN利用時の注意事項を追記 ・参考資料として「企業等が安心して無線LANを利用するために」も追記する	無線LANの導入・運用時のセキュリティ対策の考え方を追加検討する。
26	「3.6.1 コンピュータ及びネットワークの管理」	クラウドの仮想ネットワークのセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	クラウドサービス提供における情報セキュリティ対策ガイド(平成26年4月総務省) 13.1.4	仮想ネットワークの複雑な構成や設定に伴う管理ミスを防止する措置を講じることが望ましい。	明確化	62	・現行ポリシーガイドライン「3.6.1.コンピュータ及びネットワークの管理(P62)(解説)」にクラウド上の仮想ネットワークを利用する場合に、物理ネットワークと仮想ネットワークの対応関係の明確化や仮想ネットワークの運用設定方針、設定承認方針の作成について追記	クラウドの仮想ネットワークのセキュリティ対策の考え方を追加検討する。

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
27	「3.6.1 コンピュータ及びネットワークの管理」	スマートフォンのアプリケーションの入手に関するセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	スマートフォン・クラウドセキュリティ研究会最終報告会（総務省平成24年6月29日）	スマートフォンのアプリケーションの入手に注意を払うことが望ましい。	管理強化	60	現行のポリシーガイドライン(P60)に新規項目として、スマートフォンの利用におけるセキュリティ対策（アプリケーションの入手等）について追記する	スマートフォンのアプリケーションの入手に関するセキュリティ対策の考え方を追加検討する。
28	「3.6.1 コンピュータ及びネットワークの管理」	複合機のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 7.1.3	「複合機対策」 ・複合機調達の際には、セキュリティ要件を策定すること ・複合機が備える機能について、適切なセキュリティ設定を行う ・複合機の運用終了時に、電磁的記憶媒体の情報の抹消	明確化	60	現行のポリシーガイドライン(P60)に複合機を利用する場合のセキュリティ対策について追記する	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、複合機のセキュリティ要件、セキュリティ設定、セキュリティ運用の観点を追加検討する
29	「3.6.1 コンピュータ及びネットワークの管理」	特定用途機器のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 7.1.3	「特定用途機器対策」 特定用途機器について、取り扱う情報、利用方法、通信回線の形態等に脅威がある場合は、特性に応じた対応を行うこと	明確化	60	現行のポリシーガイドライン(P60)に特定用途機器を利用する場合のセキュリティ対策について追記する	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、特定用途機器のセキュリティ要件、セキュリティ設定、セキュリティ運用の観点を追加検討する
30	「3.6.1 コンピュータ及びネットワークの管理」	電子メールの利用制限	－	地方公共団体が発信する電子メールのなりすまし対策の実施について（依頼） 平成23年8月25日	電子メールの送信に使われる通信方式（SMTP)における送信者のアドレスの詐称（なりすまし）事案の多発に伴う電子メールの成りすまし対策（送信ドメイン認証技術の利用）の実施依頼のため	明確化	62	・現行ポリシーガイドライン「3.6.1.コンピュータ及びネットワークの管理(P62)(解説)」に、電子メールの成りすまし対策（送信ドメイン認証技術）について追記	平成22年10月以降の事務連絡に基づく検討事項
31	「3.6.1 コンピュータ及びネットワークの管理」	電子メールの利用制限	－	グループメールサービスの使用について（注意喚起） 平成25年7月11日	政府機関において民間企業の提供する無料のグループメールサービスを利用した結果、メールの内容が外部から閲覧可能な状態となり、必要なセキュリティが確保されなかった事案の発生に伴う注意喚起のため	明確化	62	・現行のポリシーガイドライン「3.6.1.コンピュータ及びネットワークの管理(P62)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項
32	「3.6.2 アクセス制御」	現行の情報セキュリティポリシーガイドラインには、ネットワークからのログイン制限に関する観点が弱いため	現行の情報セキュリティポリシー運用上の課題	府省庁対策基準策定のためのガイドライン 6.1.3	（ネットワークからのログイン制限） ネットワークからのログインを制限すること 例えば、電子証明書による端末認証、IPアドレス、MACアドレス等によって制限することができる	明確化	65	現行のポリシーガイドライン(P65（2）、（3）)に端末認証、IPアドレス、MACアドレス認証について追記する また、LGWANのルールとの整合が取れる形で追記する	ネットワークからのログイン制限に関する観点から見直し検討する
33	「3.6.2 アクセス制御」	現行の情報セキュリティポリシーガイドラインには、初期設定の認識コートの変更に関する観点が弱いため	現行の情報セキュリティポリシー運用上の課題	府省庁対策基準策定のためのガイドライン 6.1.3	初期設定の識別コードを変更できる場合には、識別コードを 初期設定以外のものに変更すること	明確化	64	現行のポリシーガイドライン(P64)に利用者ID付与時の順守事項について追記する	初期設定の識別コード変更に関する観点から、見直し検討を行う
34	「3.6.3 システム開発、導入、保守等」	バックアップの実施	－	ホスティングサービス等利用時におけるデータ消失等事象への対策実施及び契約内容の再確認等について（注意喚起） 平成24年7月6日	サービス利用形態や運用状況に応じた適切なバックアップの必要性について検討することが望ましい。	明確化	60	・現行のポリシーガイドライン「3.6.1.コンピュータ及びネットワークの管理(P60)(解説)」に、参照事例として、該当する通知文を参照することを追記 ・クラウド環境に対応したバックアップについて追記すべきである	平成22年10月以降の事務連絡に基づく検討事項

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
35	「3.6.3 システム開発、導入、保守等」	セキュリティに配慮した開発のための指針の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.14.2.1	ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用しなければならない	明確化	68	・現行のポリシーガイドライン(P68(2))に、セキュリティに配慮したシステムの開発方針を確立することを追記する（参照：ISO/IEC27002:2013（14.2.1））	セキュリティを配慮したソフトウェア及びシステムの開発のための規則の考え方を検討する
36	「3.6.3 システム開発、導入、保守等」	セキュリティに配慮したシステム構築の指針の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.14.2.5	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用しなければならない	管理強化	68	・現行のポリシーガイドライン(P68(2))に、システムの開発手順を確立し、文書化することを追記する ・開発手順（構築手順）が一定のセキュリティレベルを満たし、最新化されていることを確実にするため、定期的にレビューを行うことを追記する	セキュリティに配慮したシステムを構築するための原則の考え方を検討する
37	「3.6.3 システム開発、導入、保守等」	セキュリティに配慮したシステム開発環境の指針の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.14.2.6	組織は、全てのシステム開発ライフサイクルを含む。システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護しなければならない	管理強化	68	・現行のポリシーガイドライン(P68(2))に、システムの開発環境を確立する際のセキュリティ配慮について追記する（参照：ISO/IEC27002:2013（14.2.6））	システム開発ライフサイクルを含むシステムの開発開発環境の考え方を検討する
38	「3.6.3 システム開発、導入、保守等」	セキュリティ機能の試験の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.14.2.8	セキュリティ機能（functionality）の試験は、開発期間中に実施しなければならない	明確化	69	・現行のポリシーガイドライン(P69(3)②)に、組織内で開発したシステム、外部委託したシステムのそれぞれについて独立した受け入れ試験を行うことを追記する	システム開発期間中のセキュリティ機能試験の考え方を検討する
39	「3.6.3 システム開発、導入、保守等」	情報処理施設の可用性に関する観点が、見当たらないため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.17.2.1	情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない	管理強化	69	・現行のポリシーガイドライン(P69)に、情報システムの冗長性を組み入れること、完全性・機密性に対するリスクが生じることを考慮すること、等を追記する	情報処理施設の可用性の観点を追加検討する
40	「3.6.3 システム開発、導入、保守等」	情報処理施設の可用性に関する観点が、見当たらないため	今後検討すべき情報セキュリティポリシーの課題	クラウドサービス提供における情報セキュリティ対策ガイド(平成26年4月総務省) 17.2.1	情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入することが望ましい	管理強化	69	現行のポリシーガイドライン(P69(3))に、情報システムの障害発生リスクを考慮することと、システムは冗長性を持たせることについて追記する	情報処理施設の可用性の観点を追加検討する
41	「3.6.5 不正アクセス対策」	現行の情報セキュリティポリシーガイドラインには、大規模な障害・事故等に関する連絡網や体制に観点が弱いため	現行の情報セキュリティポリシー運用上の課題	NISC統一基準（平成26年度版） 2.2.4	緊急連絡網には当該システムに係る責任者及び管理者のほか、大規模な障害・事故等に備えて最高情報セキュリティ責任者も含める必要がある	明確化	76	現行のポリシーガイドライン(P76)に、インシデント発生時の緊急連絡網について強調するためにも追記する	大規模な障害・事故等に備えての体制、連絡網の観点で見直し検討する
42	「3.6.5 不正アクセス対策」	現行の情報セキュリティポリシーガイドラインには、現場でのセキュリティ事件・事故対応に関する体制の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	構成員からのご意見	各団体の現場でセキュリティ事件や事故等の対応ができる仕組み（CSIRT：ComputerSecurityIncidentResponseTeam）が必要である	管理強化	77	・現行のポリシーガイドライン「3.6.5.不正アクセス対策(P76-77)(例文、解説)」に、【推奨事項】としてCSIRTと連携した監視、通知、適切な対応などについて追記	各団体の現場でセキュリティ事件や事故等の対応ができる仕組み（CSIRT：ComputerSecurityIncidentResponseTeam）作りの観点で見直し検討する
43	「3.6.5 不正アクセス対策」	USBメモリ等の外部記憶媒体等のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 8.1.1	USBメモリ等の外部電磁記録媒体を用いた利用基準をきめること (a)支給の媒体を利用する（私物や出所不明の媒体を使用しない） (b)紛失・盗難リスク防止 (c)セキュアな外部媒体の利用（暗号化）	明確化	76	現行のポリシーガイドライン(P76)に不正アクセスに対するシステム・ルール的な対策について追記する（関係ページへの参照等も検討する）	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、USBメモリ等の外部電磁記録媒体を用いた利用基準の観点を追加検討する

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
44	「3.6.5 不正アクセス対策」	支給品以外の端末利用に関するセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 8.2	「支給以外の端末の利用」 端末に情報を保存させず、支給以外の端末を業務利用することを可能とする。仕組みとして、シンクライアントやリモートデスクトップの技術の活用が有効	明確化	76	現行のポリシーガイドライン(P76)に不正アクセスに対するシステム・ルール的な対策について追記する（関係ページへの参照等も検討する）	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、支給品以外の端末の利用時のセキュリティ対策の観点を追加検討する
45	「3.6.5 不正アクセス対策」	ソーシャルメディアサービスによる情報発信に関するセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 4.1.3	（ソーシャルメディアサービスによる情報発信） (a)アカウントによる情報発信が本物か、成りすまし対策を講ずること (b)パスワード等の生体認証情報を適切に管理するなどの不正アクセス対策を実施すること 情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含めなければならない。	明確化	76	現行のポリシーガイドライン(P76)に不正アクセスに対するシステム・ルール的な対策について追記する（関係ページへの参照等も検討する）	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、ソーシャルメディアサービスによる情報発信時の対策等を検討する
46	「3.6.5 不正アクセス対策」	標的型攻撃に対する対策の考え方が弱いため	今後検討すべき情報セキュリティポリシーの課題	府省庁対策基準策定のためのガイドライン 6.2.4	標的型攻撃対策の実施 (a)入口対策 (b)侵入後の早期検知、改ざん防止	管理強化	76	現行のポリシーガイドライン(P76)に 標的型攻撃対策（入口対策、オートラン無効化、USBポート無効化、検知、対処）を追記する	新しいNISC統一基準（平成26年度版）の改定状況を見ながら、従来の不正アクセス対策に、標的型対策を含めた考え方を追加検討する
47	「3.6.5 不正アクセス対策」	スマートフォンのOS更新やウィルス対策ソフトに関するセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	スマートフォン・クラウドセキュリティ研究会最終報告会（総務省平成24年6月29日）	よりスマートフォン情報セキュリティ3か条 「1．OS（基本ソフト）の更新」 「2．ウイルス対策ソフトの確認」	管理強化	76	現行のポリシーガイドライン(P76)に新規項目として、スマートフォンの利用におけるセキュリティ対策（OS更新、ウイルス対策ソフトの確認等）について追記する	スマートフォンのOS更新やウイルス対策ソフトに関するセキュリティ対策の考え方を追加検討する。
48	「3.6.5 不正アクセス対策」	情報セキュリティインシデントからの対応力の考え方が弱いため	今後検討すべき情報セキュリティポリシーの課題	構成員からのご意見	ISMSやNISCの改定差分の反映だけでは、新たなセキュリティリスクに対して、後追いになるおそれがある	—	—	・今回の改定では、以下の2つの考え方を組み合わせることにより、①セキュリティ対策の網羅性を高め、②セキュリティインシデント対応力の強化を行う。 ①ISMSやNISC等の差分をもとにした改定 ②過去の事故事例や注意喚起通知を活用した改定 ※ガイドライン改定全体に関する事項であり、本項目に関する個別の改定はなし	2本立ての考え方で対応する。1つはISMSやNISC等の差分を見ることでセキュリティ対策の網羅性を高める。もう1つは、ISMSの「情報セキュリティインシデントからの学習」を導入し、セキュリティ事件や事故事例（注意喚起等の通達文）を活用し、新たなセキュリティインシデントに対しても対応力を高める方向で検討する
49	「3.6.5 不正アクセス対策」	標的型攻撃のような最近のセキュリティ事故に対する対策の考え方が弱いため	今後検討すべき情報セキュリティポリシーの課題	構成員からのご意見	最近の標的型攻撃は被害範囲と頻度が増大しているため、従来のやり方では対応できないおそれがある	管理強化	76-77	・現行のポリシーガイドライン「3.6.5.不正アクセス対策(P76-77)(例文、解説)」に、【推奨事項】としてCSIRTと連携した監視、通知、適切な対応などについて追記、また、適切なログの管理、管理者権限管理、自治体CEPTERでの情報共有などについて追記	自治体CEPTOARによる情報共有の有効活用とNISCで検討している標的型攻撃対策の考え方を追加検討する
50	「3.6.6 セキュリティ情報の収集」	技術的脆弱性の管理 技術的脆弱性の悪用を防止するため	—	JavaSE6のサポート有効期間の満了に係る対応について（注意喚起） 平成24年7月24日	JavaSE6のサポート有効期間の満了に伴い、H24.12以降に修正プログラムの提供が行われなくなることへの対応	明確化	79	・現行のポリシーガイドライン「3.6.6.セキュリティ情報の収集(P79)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項
51	「3.6.6 セキュリティ情報の収集」	技術的脆弱性の管理 技術的脆弱性の悪用を防止するため	—	JavaSE6のサポート有効期間の3か月間延長及びサポート満了に伴う対応について（再周知・注意喚起） 平成24年8月15日	JavaSE6のサポート有効期間が平成24年11月末から平成25年2月末へ3か月延長されることに伴う対応	明確化	79	・現行のポリシーガイドライン「3.6.6.セキュリティ情報の収集(P79)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
52	「3.6.6 セキュリティ情報の収集」	技術的脆弱性の管理 技術的脆弱性の悪用を防止するため	―	WindowsXP等のサポート有効期間の満了に係る対応について（注意喚起） 平成25年4月22日	WindowsXP、Office2003、InternetExplorer6の製品サポート終了（H26.4.9終了）に伴う適切な対応	明確化	79	・現行のポリシーガイドライン「3.6.6.セキュリティ情報の収集(P79)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項
53	「3.6.6 セキュリティ情報の収集」	技術的脆弱性の管理 技術的脆弱性の悪用を防止するため	―	WindowsXP等のサポート有効期間の満了に係る対応について 平成25年11月22日	WindowsXP、Office2003、InternetExplorer6の製品サポート終了（H26.4.9終了）に伴う適切な対応	明確化	79	・現行のポリシーガイドライン「3.6.6.セキュリティ情報の収集(P79)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項
54	「3.6.6 セキュリティ情報の収集」	技術的脆弱性の管理 技術的脆弱性の悪用を防止するため	―	WindowsXP等のサポート期間の終了に伴う対応について 平成26年4月11日	WindowsXP、Office2003、InternetExplorer6の製品サポート終了（H26.4.9終了）に伴う適切な対応	明確化	79	・現行のポリシーガイドライン「3.6.6.セキュリティ情報の収集(P79)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項
55	「3.7.1 情報システムの監視」	職員や委託先の従業員における内部不正に対する記述が弱いため	今後検討すべき情報セキュリティポリシーの課題	組織における内部不正防止ガイドライン（情報処理推進機構） （18）	システム管理者のアクセス履歴や操作履歴等のログ・証跡を保管し、内容を定期的にシステム管理者以外が確認する	明確化	80	・現行のポリシーガイドライン「3.7.1.情報システムの監視(P80)(解説)」に特権を付与されたIDのログについて確実にログの確認を定期的に行うよう記述を強化する。	組織における内部不正に対するガイドラインに基づく検討事項
56	「3.7.3 侵害時の対応」	情報セキュリティ事象の評価部分の記述が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.16.1.4	情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定しなければならない	明確化	83	・現行のポリシーガイドライン(P83)に、情報資産に対する侵害事案が発生した場合の、事象の分類の検討について追記する	情報セキュリティインシデント発生時の評価及び対応を追加検討する
57	「3.7.3 侵害時の対応」	情報セキュリティインシデントからの対応力の考え方が弱いため	今後検討すべき情報セキュリティポリシーの課題	構成員からのご意見	ISMSやNISCの改定差分の反映だけでは、新たなセキュリティリスクに対して、後追いになるおそれがある	―	―	・今回の改定では、以下の2つの考え方を組み合わせることにより、①セキュリティ対策の網羅性を高め、②セキュリティインシデント対応力の強化を行う。 ①ISMSやNISC等の差分をもとにした改定 ②過去の事故事例や注意喚起通知を活用した改定 ※ガイドライン改定全体に関する事項であり、本項目に関する個別の改定はなし	2本立ての考え方で対応する。1つはISMSやNISC等の差分を見ることでセキュリティ対策の網羅性を高める。もう1つは、ISMSの「情報セキュリティインシデントからの学習」を導入し、セキュリティ事件や事故事例（注意喚起等の通達文）を活用し、新たなセキュリティインシデントに対しても対応力を高める方向で検討する
58	「3.7.3 侵害時の対応」	標的型攻撃のような最近のセキュリティ事故に対する対策の考え方が弱いため	今後検討すべき情報セキュリティポリシーの課題	構成員からのご意見	最近の標的型攻撃は被害範囲と頻度が増大しているため、従来のやり方では対応できないおそれがある	管理強化	84	・現行ガイドライン「3.7.3侵害時の対応（P84)(解説)」の(1)においてCSIRTとの連携や、自治体CEPTER内での情報共有を行うことを追記	自治体CEPTOARによる情報共有の有効活用とNISCで検討している標的型攻撃対策の考え方を追加検討する
59	「3.7.3 侵害時の対応」	情報セキュリティインシデントの管理及びその改善 セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため	―	地方公共団体における情報セキュリティ対策及び政府等との情報共有の一層の充実・強化について（依頼） 平成23年10月11日	政府等との情報共有の一層の充実・強化のため	明確化	84	・現行ガイドライン「3.7.3侵害時の対応（P84)(解説)」の(2)①の「関係機関」に説明と参考資料として該当する通知文を参照することを追加	政府等との情報共有の一層の充実・強化について追記する （平成22年10月以降の事務連絡）

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
60	「3.7.4 外部委託」	外部委託の要求事項に、供給者のアクセスに関連する観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.15.1.1	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化しなければならない	明確化	87	・現行のポリシーガイドライン(P87)に、組織へICTサービスを提供する供給者が情報にアクセスする場合の合意について追記する（参考：ISO/IEC27002:2013（15.1.1））	外部委託の要求事項に、供給者のアクセスに関するリスク低減の観点を追加検討する
61	「3.7.4 外部委託」	外部委託の要求事項に、ICTサービスや製品のサプライチェーンの観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.15.1.3	供給者との合意には、情報通信技術（ICT）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない	明確化	87	・現行のポリシーガイドライン(P87)に、組織へICTサービスを提供する供給者のサプライチェーンに対するセキュリティについて、供給者との合意を行う事項を追記する（参考：ISO/IEC27002:2013（15.1.3））	外部委託の要求事項に、ICTサービスや製品のサプライチェーンの観点を追加検討する
62	「3.7.4 外部委託」	外部委託の要求事項に、ICTサービスや製品のサプライチェーンの観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	クラウドサービス提供における情報セキュリティ対策ガイド（平成26年4月総務省） 15.1.3	供給者との合意には、情報通信技術（以下ICTという）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい	明確化	87	・現行のポリシーガイドライン(P87)に、クラウドサービスを利用する場合の、ICTサプライチェーンのおけるセキュリティ対策の確認と選択について追記する	外部委託の要求事項に、ICTサービスや製品のサプライチェーンの観点を追加検討する
63	「3.7.4 外部委託」	現行の情報セキュリティポリシーガイドラインには、海外のデータセンター等の利用に関する観点が弱いため	現行の情報セキュリティポリシー運用上の課題	府省庁対策基準策定のためのガイドライン 4.1.1	（外部委託管理） データの所在については、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、不適切となるアクセスをされる可能性があることに注意が必要である	明確化	90	現行のポリシーガイドライン(P90（注6）)に海外DCの話が記載されているが、現在の「ASP・SaaS」だけでなく、「外部委託」「クラウド」といった観点で説明できるよう、範囲を広げた形で修正を行う	（外部委託管理） 海外のデータセンター等に情報を保存する場合等の観点で、見直しを検討する
64	「3.7.4 外部委託」	供給者関係における情報セキュリティ 供給者がアクセスできる組織の資産の保護を確実にするため	—	ホスティングサービス等利用時におけるデータ消失等事象への対策実施及び契約内容の再確認等について（注意喚起） 平成24年7月6日	情報システムの重要性を踏まえた適切なバックアップが講じられているか（本番データとバックアップデータが同時消失することがないか等）、について適切な契約内容となっていることが必要。（現状確認含む）	明確化	90	・現行のポリシーガイドライン(P90)において、参考資料として「地方公共団体におけるASP・SaaSの導入・活用に関するガイドライン」が記載されているが、追加として「外部委託における情報セキュリティ対策実施規程 雛形付録」(NISC)を追記する	平成22年10月以降の事務連絡に基づく検討事項
65	「3.7.4 外部委託」	外部委託の要求事項に、再委託の観点が弱いため	—	地方公共団体が保有する個人情報の適切な管理の徹底について（注意喚起） 平成26年7月28日	再委託先についても委託先同様の情報セキュリティ対策が実施されていることを担保することが必要である	明確化	89	・現行のポリシーガイドライン(P89)において、再委託を行う場合についても委託先と同等の情報セキュリティ対策が行われていることを委託元に担保させることを追記する	平成22年10月以降の事務連絡に基づく検討事項
66	「3.7.6　法令遵守」	現行の情報セキュリティポリシーガイドラインには、海外のデータセンター等の利用に関する観点が弱いため	現行の情報セキュリティポリシー運用上の課題	府省庁対策基準策定のためのガイドライン 4.1.1	（外部委託管理） データの所在については、海外のデータセンター等に情報を保存する場合には、保存している情報に対し、現地の法令等が適用されるため、不適切となるアクセスをされる可能性があることに注意が必要である	明確化	92	現行ポリシーガイドライン(P92)は法令順守についての項目であるが、「外部委託」「クラウド」利用の際の海外DC利用についての注意喚起するための修正を行う	（外部委託管理） 海外のデータセンター等に情報を保存する場合等の観点で、見直しを検討する
67	「3.7.6　法令遵守」	クラウドサービスの提供を受ける場合、各国の適用法や司法権の管轄などが異なる等の、クラウドサービス等のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A18.1.1	各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保たなければならない。	管理強化	92	・現行のポリシーガイドライン(P92)に、法令を遵守するための具体的な管理策及び責任について文書化し、管理することを追記する	クラウドサービス等各国の適用法等のセキュリティ対策の考え方を追加検討する。

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
68	「3.7.6 法令遵守」	クラウドサービスの提供を受ける場合、各国の適用法や司法権の管轄などが異なる等の、クラウドサービス等のセキュリティ対策の観点が弱いため	今後検討すべき情報セキュリティポリシーの課題	クラウドサービス提供における情報セキュリティ対策ガイド(平成26年4月総務省) 18.1.1	各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つことが望ましい。	管理強化	92	・現行のポリシーガイドライン(P92)に、クラウドサービスを利用する場合の、情報の保管先について把握し、海外データセンターの場合はその国の法令の適用を受ける旨を追記し、注意喚起を行う	クラウドサービス等各国の適用法等のセキュリティ対策の考え方を追加検討する。
69	「3.8 評価・見直し」	現行の情報セキュリティポリシーガイドラインには、監査結果や点検結果を元にした見直し(リスク分析、セキュリティポリシー、実施手順等)の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	定期的な監査・点検は、約40%の団体が実施しており、定着しつつあるものの、監査結果や点検結果を元にした見直しが実施されていない課題がある	明確化	94	・現行ポリシーガイドライン「3.8.1.監査(P94)」に、監査を実施する上での参考資料として「地方公共団体における情報セキュリティ監査に関するガイドライン」を追記する（P96注3に記載があるが、より強調するよう、記載箇所を移動する）	監査や点検実施後の一連の対応が実施できている団体の進め方、体制、事例なども参考にしながら、情報セキュリティ対策の見直しを徹底する観点で、検討を行う
70	「3.8 評価・見直し」	定期的な監査・点検を実施し、情報セキュリティ対策を見直す必要がある	—	地方公共団体の保有する情報資産の管理状況等の再点検について（依頼） 平成24年10月29日	地方公共団体の保有する個人情報の人的な要因による漏えい事案や、団体職員の不正行為により個人情報が漏えいする事案の発生を踏まえた再点検	明確化	98	・現行のポリシーガイドライン「3.8.2.自己点検(P98)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項
71	「3.8 評価・見直し」	定期的な監査・点検を実施し、情報セキュリティ対策を見直す必要がある	—	地方公共団体における個人情報の漏洩防止対策について（注意喚起） 平成25年8月5日	「地方公共団体の保有する情報資産の管理状況等の再点検について（依頼）24.10.29」の注意喚起	明確化	98	・現行のポリシーガイドライン「3.8.2.自己点検(P98)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項
72	「3.8 評価・見直し」	技術的脆弱性の管理 技術的脆弱性の悪用を防止するため	—	地方公共団体等が管理するウェブサイトに係る脆弱性の確認及び対策の点検・実施等について（依頼） 平成24年9月26日	H24.9中旬に複数の地方公共団体のほか、政府機関等における情報システムの一部ウェブサイトに対する外部からの攻撃により、改ざんや一時閲覧困難となった事案が確認されており、NISCより各府省庁に対し、政府機関等が管理するウェブサイトに係る脆弱性の確認及び対策の点検・実施の依頼があったため	明確化	98	・現行のポリシーガイドライン「3.8.2.自己点検(P98)(解説)」に、参照事例として、該当する通知文を参照することを追記	平成22年10月以降の事務連絡に基づく検討事項
73	「3.8.3 情報セキュリティポリシーの見直し」	セキュリティ基本方針のレビューだけでは、最近の事案には対応できず、拡大する必要があるため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.5.1.1	情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知しなければならない	明確化	99	・現行のポリシーガイドライン(P99)に、情報セキュリティポリシーの見直し時に含めるべき観点を追記する ・事業戦略 ・規制、法令及び契約 ・現在及び予想される情報セキュリティの脅威環境 ・個別方針の例を追記する	情報セキュリティのための方針群（モバイル機器、アクセス制御、ネットワーク及びネットワークサービス、暗号により管理策、鍵管理）の考え方を追加検討する。
74	「3.8.3 情報セキュリティポリシーの見直し」	セキュリティ基本方針のレビューだけでは、最近の事案には対応できず、拡大する必要があるため	今後検討すべき情報セキュリティポリシーの課題	ISO/IEC27001:2013 A.5.1.2	情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューしなければならない	明確化	99	・現行のポリシーガイドライン(P99)に、情報セキュリティポリシーの見直し頻度や見直し手順について追記する ※重大な変化が発生した際に実施する ※組織環境、業務環境、法的状況等の変化に応じた情報セキュリティのための方針や取組に関する改善の機会の評価を含める	情報セキュリティのための方針群（モバイル機器、アクセス制御、ネットワーク及びネットワークサービス、暗号により管理策、鍵管理）の考え方を追加検討する。
75	「権限・責任等一覧表」	現行の情報セキュリティポリシーガイドラインには、「権限・責任者一覧」が添付されているが、利用方法が分かりにくいため	現行の情報セキュリティポリシー運用上の課題	構成員からのご意見	ポリシーガイドラインの対象者が誰かを明確化させ、ポリシーガイドラインの記述内容を明確化する必要がある	—	—	・ポリシーガイドラインの想定する読者や読者のスキルレベルを「1.1.本ガイドラインの目的」に記載する ・権限・責任等一覧表の修正はなし	「権限・責任等一覧表」等をうまく活用しながら、ポリシーガイドライン上の対象者を明確化する観点で、検討を行う
76	「地方公共団体における情報セキュリティ監査ガイドライン（平成22年11月）」	現行の情報セキュリティポリシーガイドラインには、監査結果や点検結果を元にした見直し(リスク分析、セキュリティポリシー、実施手順等)の観点が弱いため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	定期的な監査・点検は、約40%の団体が実施しており、定着しつつあるものの、監査結果や点検結果を元にした見直しが実施されていない課題がある	—	—	・現行ポリシーガイドライン「1.8.1.監査・自己点検(P13)」と「3.8.1.監査(P94)」において、監査実施する上での参考資料として「地方公共団体における情報セキュリティ監査に関するガイドライン」を追記する	監査や点検実施後の一連の対応が実施できている団体の進め方、体制、事例なども参考にしながら、情報セキュリティ対策の見直しを徹底する観点で、検討を行う

【資料2－3】ガイドライン改訂に向けた論点整理表

2014/09/26

項番	ガイドライン等の対象箇所	改定の理由	改定分類	改定の要求元とその背景		改定方針			
				要求元	改定の背景	区分	対象ページ	改定方針 （改定是非、改定レベル）	（参考 前フェーズ検討結果） 改定の方向性
77	参考資料「地方公共団体における情報資産のリスク分析・評価に関する手引き（平成21年3月）」	リスク分析の実施に関しては、「地方公共団体における情報資産のリスク分析・評価に関する手引き（平成21年3月）」が参照されているが、実施方法に関して見直す必要があるため	現行の情報セキュリティポリシー運用上の課題	運用上の課題	主要な情報資産について調査及びリスク分析は、（地方自治情報管理概要の平成25年度によると）都道府県では約60%、市区町村は約30%の実施率にとどまっており、実施できない理由に難しさと時間がかかる点をあげている	—	—	・現行のポリシーガイドライン「1.6.4.リスク分析の実施(P10)」に、簡易リスク分析方法等についての追記修正を行う ・手引き自体の修正はなし	簡易リスク分析等を含めた、現場で実施しやすいリスク分析の方法を検討する