○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（案） 新旧対照表

改定案	現行
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	政府機関等の情報セキュリティ対策のための統一規範
平成 28 年８月 31 日 平成 30 年７月 25 日改定 平成 31 年４月１日改定 令和３年×月×日改定 サイバーセキュリティ戦略本部決定	平成 28 年８月 31 日 平成 30 年７月 25 日改定 平成 31 年４月１日改定 サイバーセキュリティ戦略本部決定
第一章　目的及び適用対象（第一条―第二条） 第二章　政府機関等の情報セキュリティ対策のための基本方針（第三条―第四条） 第三章　政府機関等の情報セキュリティ対策のための基本対策（第五条―第二十三条） 附則	第一章　目的及び適用対象（第一条―第二条） 第二章　政府機関等の情報セキュリティ対策のための基本方針（第三条―第四条） 第三章　政府機関等の情報セキュリティ対策のための基本対策（第五条―第二十三条） 附則
第一章　目的及び適用対象	第一章　目的及び適用対象
（目的） 第一条　（略）	（目的） 第一条　（略）
（適用対象） 第二条　本規範の適用対象とする組織は、次の各号に掲げるとおりとする。 一　国の行政機関　法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関	（適用対象） 第二条　本規範の適用対象とする組織は、次の各号に掲げるとおりとする。 一　国の行政機関　法律の規定に基づき内閣に置かれる機関若しくは内閣の所轄の下に置かれる機関、宮内庁、内閣府設置法（平成十一年法律第八十九号）第四十九条第一項若しくは第二項に規定する機関、国家行政組織法（昭和二十三年法律第百二十号）第三条第二項に規定する機関又はこれらに置かれる機関

改定案	現行
二　独立行政法人　独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人 三　指定法人　法第十三条に規定する指定法人 2　本規範の適用対象とする者は、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。 3　本規範の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）及び情報システムの設計又は運用管理に関する情報とする。	二　独立行政法人　独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する法人 三　指定法人　法第十三条に規定する指定法人 2　本規範の適用対象とする者は、国の行政機関において行政事務に従事している国家公務員、独立行政法人及び指定法人において当該法人の業務に従事している役職員その他機関等の指揮命令に服している者であって、次項に規定する情報を取り扱う者（以下「職員等」という。）とする。 3　本規範の適用対象とする情報は、職員等が職務上取り扱う情報であって、情報処理若しくは通信の用に供するシステム（以下「情報システム」という。）又は外部電磁的記録媒体に記録された情報及び情報システムの設計又は運用管理に関する情報とする。
第二章　政府機関等の情報セキュリティ対策のための基本方針	第二章　政府機関等の情報セキュリティ対策のための基本方針
（リスク評価と対策） 第三条　（略）	（リスク評価と対策） 第三条　（略）
（情報セキュリティ文書） 第四条　機関等は、自組織の特性を踏まえ、基本方針（機関等における情報セキュリティ対策の基本的な方針をいう。以下同じ。）及び対策基準（機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。以下同じ。）を定めなければならない。基本方針及び対策基準（以下「ポリシー」という。）の呼称は機関等で独自に定めることができる。 2　基本方針は、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目的、対象範囲等の情報セキュリティに対する基本的な考え方を定めなければならない。 3　対策基準は、別に定める政府機関等のサイバーセキュリティ対策のための統	（情報セキュリティ文書） 第四条　機関等は、自組織の特性を踏まえ、基本方針（機関等における情報セキュリティ対策の基本的な方針をいう。以下同じ。）及び対策基準（機関等における情報及び情報システムの情報セキュリティを確保するための情報セキュリティ対策の基準をいう。以下同じ。）を定めなければならない。基本方針及び対策基準（以下「ポリシー」という。）の呼称は機関等で独自に定めることができる。 2　基本方針は、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目的、対象範囲等の情報セキュリティに対する基本的な考え方を定めなければならない。 3　対策基準は、別に定める政府機関等の情報セキュリティ対策のための統一基

改定案	現行
一基準（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるように定めなければならない。 4　国の行政機関は、必要に応じて、所管する独立行政法人及び指定法人に対して、自らのポリシーを当該法人がポリシーを定める際に参照するよう求めることとする。 5　独立行政法人及び指定法人は、前項の求めに応じることとする。 6　機関等は、前条第一項の評価結果を踏まえ、ポリシーの評価及び見直しを行わなければならない。	準（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるように定めなければならない。 4　国の行政機関は、必要に応じて、所管する独立行政法人及び指定法人に対して、自らのポリシーを当該法人がポリシーを定める際に参照するよう求めることとする。 5　独立行政法人及び指定法人は、前項の求めに応じることとする。 6　機関等は、前条第一項の評価結果を踏まえ、ポリシーの評価及び見直しを行わなければならない。
第三章　政府機関等の情報セキュリティ対策のための基本対策	第三章　政府機関等の情報セキュリティ対策のための基本対策
（管理体制） 第五条　（略）	（管理体制） 第五条　（略）
（対策推進計画） 第六条　（略）	（対策推進計画） 第六条　（略）
（例外措置） 第七条　（略）	（例外措置） 第七条　（略）
（教育） 第八条　（略）	（教育） 第八条　（略）
（情報セキュリティインシデントへの対応） 第九条　機関等は、情報セキュリティインシデント（JIS Q 27000:2019における情報セキュリティインシデントをいう。以下同じ。）に対処するため、適正な体制を構築するとともに、必要な措置を定め、実施しなければならない。 2　情報セキュリティインシデントの可能性を認知した者は、ポリシーに定める報告窓口に報告しなければならない。	（情報セキュリティインシデントへの対応） 第九条　機関等は、情報セキュリティインシデント（JIS Q 27000:2014における情報セキュリティインシデントをいう。以下同じ。）に対処するため、適正な体制を構築するとともに、必要な措置を定め、実施しなければならない。 2　情報セキュリティインシデントの可能性を認知した者は、ポリシーに定める報告窓口に報告しなければならない。

改定案	現行
3　ポリシーに定める責任者は、情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じなければならない。	3　ポリシーに定める責任者は、情報セキュリティインシデントに関して報告を受け又は認知したときは、必要な措置を講じなければならない。
（自己点検） 第十条　（略）	（自己点検） 第十条　（略）
（監査） 第十一条　（略）	（監査） 第十一条　（略）
（情報の格付） 第十二条　（略）	（情報の格付） 第十二条　（略）
（情報の取扱制限） 第十三条　（略）	（情報の取扱制限） 第十三条　（略）
（情報のライフサイクル管理） 第十四条　（略）	（情報のライフサイクル管理） 第十四条　（略）
（情報を取り扱う区域） 第十五条　（略）	（情報を取り扱う区域） 第十五条　（略）
（外部委託） 第十六条　機関等は、情報処理に係る業務を外部委託する場合には、必要な措置を定め、実施しなければならない。	（外部委託） 第十六条　機関等は、情報処理に係る業務を外部委託する場合には、必要な措置を定め、実施しなければならない。
2　機関等は、外部委託を実施する際に要機密情報を取り扱う場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めなければならない。	2　機関等は、外部委託（約款による外部サービスの利用を除く。）を実施する場合は、委託先において情報漏えい対策や、委託内容に意図しない変更が加えられない管理を行うこと等の必要な情報セキュリティ対策が実施されることを選定条件とし、仕様内容にも含めなければならない。
（削る）	3　機関等は、要機密情報を約款による外部サービスを利用して取り扱ってはならない。

改定案	現行
3　機関等は、機器等の調達に当たり、既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処を含む選定基準を整備しなければならない。 （情報システムに係る文書及び台帳整備） 第十七条　（略） （情報システムのライフサイクル全般にわたる情報セキュリティの確保） 第十八条　（略） （情報システムの運用継続計画） 第十九条　（略） （暗号・電子署名） 第二十条　（略） （インターネット等を用いた行政サービスの提供） 第二十一条　（略） （情報システムの利用） 第二十二条　（略） （統一基準への委任） 第二十三条　（略） 附則　（略）	4　機関等は、機器等の調達に当たり、既知の脆弱性に対応していないこと、危殆化した技術を利用していること、不正プログラムを埋め込まれること等のサプライチェーン・リスクへの適切な対処を含む選定基準を整備しなければならない。 （情報システムに係る文書及び台帳整備） 第十七条　（略） （情報システムのライフサイクル全般にわたる情報セキュリティの確保） 第十八条　（略） （情報システムの運用継続計画） 第十九条　（略） （暗号・電子署名） 第二十条　（略） （インターネット等を用いた行政サービスの提供） 第二十一条　（略） （情報システムの利用） 第二十二条　（略） （統一基準への委任） 第二十三条　（略） 附則　（略）