





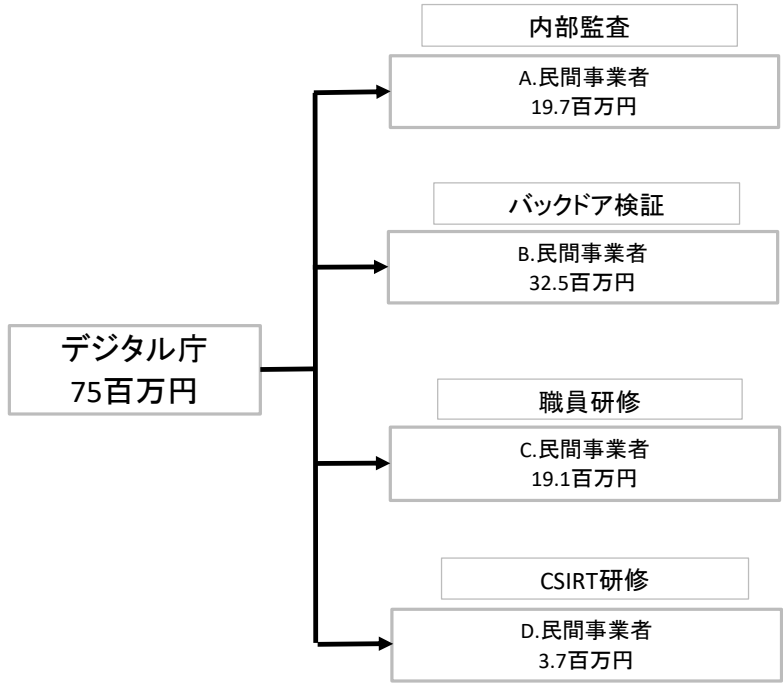
令和5年度行政事業レビューシート (デジタル庁)

事業名	サイバーセキュリティ対策等事業費			担当部局庁	戦略・組織グループ	作成責任者	
事業開始年度	令和3年度	事業終了(予定)年度	終了予定なし	担当課室	セキュリティ危機管理	参事官 松田 洋平	
会計区分	一般会計						
根拠法令 (具体的な 条項も記載)	デジタル庁設置法第4条第2項第19号 デジタル社会形成基本法第33条			関係する 計画、通知等	デジタル社会の実現に向けた重点計画(令和5年6月9日閣議決定) サイバーセキュリティ戦略(令和3年9月28日閣議決定)		
政策	デジタル社会の形成に関する施策の推進			主要経費	その他の事項経費		
施策	-						
政策体系・評価書URL	https://www.digital.go.jp/policies/assessment/						
事業の目的 (5行程度以内)	近年、システムの脆弱性やバックドア等を利用した攻撃含むセキュリティインシデントが深刻化する中、デジタル庁においても、情報システムの設計・開発段階を含めてセキュリティの強化を図ることは重要である。 特に、刻々と進化するハッカーの手法に対抗するため、ハッカーの思想を踏まえてサイバー攻撃に強いシステムを企画設計(セキュリティ・バイ・デザイン)するほか、運用・保守段階含めシステムの脆弱性を未然に発見・防止するなど、システムライフサイクル全体で対策を確実に実行することが重要である。 また、デジタル庁が整備・運用するシステムを中心とした安定的・継続的な稼働の確保等の観点から、必要な検証・監査を着実に進める。						
現状・課題 (5行程度以内)	IoT、AI等により実現されるSociety 5.0として目指すべき社会では、サイバー空間の利用は不可欠である一方、自由なアクセスやその活用を妨げるリスクが深刻化している。国民の生活や経済活動の基盤となる政府等の情報システムを含む重要インフラ等への国境を越えたサイバー攻撃は恒常的に生じており、対策の重要性はますます大きくなっているところである。また、経済社会のデジタル化が広範かつ急速に進展する中、情勢の変化に即応したサイバーセキュリティ対策を講ずることの重要性も一層高まっている。いまや、あらゆる主体がサイバー空間に参加することとなる中、デジタル化の動きと呼応し、「誰一人取り残さない」サイバーセキュリティの確保が求められている。						
事業概要 (5行程度以内)	デジタル庁の情報システムの企画・開発・整備・運用に携わる職員が各工程でセキュリティ・バイ・デザインの考え方を理解し、実務で活かすことを目的としたセキュリティ評価等のスキル形成等を実施するとともに、デジタル庁CSIRT要員が、インシデント対応に必要な機能を部外研修により習得する。 デジタル庁内のシステムの整備・運用に際して、安全性を確保するため、ソフトウェア構成管理を活用した脆弱性・バックドアへの対策を実施するとともに、デジタル庁が整備・運用するシステムについて、セキュリティポリシーに準拠した運用管理規程の策定及び当該運用管理規程に準拠した運用管理が行われているか等、セキュリティ確保に関する取組の検証・監査・調査等を実施する。						
事業概要URL	-						
実施方法	直接実施、委託・請負						
補助率等	-						
予算額・ 執行額 (単位:百万円) (インプット)	予算の 状況	当初予算(A)	令和2年度	令和3年度	令和4年度	令和5年度	令和6年度要求
		補正予算(B)	-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-
			-	-	-	-	-
		前年度から繰越し(C)	-	-	-	-	-
		翌年度へ繰越し(D)	-	-	-	-	-
		予備費等(E)	-	138	-	-	-
		計(F) =(A)+(B)+(C)+(D)+(E)	-	138	120	125	127
		執行額(G)	-	138	75	-	-
執行率(%) =(G)/(F)	-	100%	63%	-	-		
当初予算+補正予算に対する執行額の 割合(%) =(G)/[(A)+(B)]	-	-	63%	-	-		
令和5・6年度 予算内訳 (単位:百万円)	歳出予算項・目		令和5年度当初予算	令和6年度要求	主な増減理由(・要望額・予備費)		
	(項)	デジタル社会形成推進費			デジタル庁システムのサイバーセキュリティ確保のために必要な監査業務及び研修経費の増。		
	(目)	情報処理業務庁費	125	127			
		その他					
	計(A)		125	127			

活動内容① (アクティビティ)		デジタル庁の情報システムの企画・開発・整備・運用に携わる職員が各工程でセキュリティ・バイ・デザインの考え方を理解し、実務で活かす事を目的としたセキュリティ評価等のスキル形成等を実施するとともに、デジタル庁CSIRT要員が、インシデント対応に必要な識能を部外研修により習得する。								
↓										
活動目標及び活動実績① (アウトプット)		活動目標	活動指標		単位	令和2年度	令和3年度	令和4年度	5年度 活動見込	6年度 活動見込
		セキュリティバイデザインの定着に向けた研修を実施し、CSIRT職員に対しインシデント対応に必要な研修の実施	研修提供回数		回	-	-	-		
					回	-	-	-	3	5
↓										
成果目標①-1の 設定理由 (アウトプット からのつながり)										
成果目標及び成果実績①-1 (短期アウトカム)		成果目標	定量的な成果指標		単位	令和2年度	令和3年度	令和4年度	目標年度 年度	
					件	-	-	-		
					件	-	-	-		
					%	-	-	-		
成果実績及び目標値 の根拠として用いた 統計・データ名(出典) /定性的なアウトカム に関する成果実績										
↓										
成果目標①-2の 設定理由 (短期アウトカム からのつながり)										
成果目標及び成果実績①-2 (中期アウトカム)		成果目標	定量的な成果指標		単位	令和2年度	令和3年度	令和4年度	目標年度 8 年度	
					件	-	-	-		
					件	-	-	-		
					%	-	-	-		
成果実績及び目標値 の根拠として用いた 統計・データ名(出典) /定性的なアウトカム に関する成果実績										
↓										
成果目標①-3の 設定理由 (長期アウトカム へのつながり)		デジタル庁内の情報システムに携わる職員に対し、セキュリティバイデザインの定着に向けた研修を実施し、デジタル庁の情報システムの企画・開発・整備・運用における各工程でセキュリティ・バイ・デザインの考え方を浸透させる。また、デジタル庁CSIRT職員に対しインシデント対応に必要な研修実施し、情報セキュリティインシデント対応に必要な識能を習得させる。								
成果目標及び成果実績①-3 (長期アウトカム)		成果目標	定量的な成果指標		単位	令和2年度	令和3年度	令和4年度	目標最終年度 年度	
		デジタル庁システムにおける工程でのセキュリティバイデザインの浸透及びデジタル庁CSIRT職員のインシデント能力の維持・向上				-	-	-		
						-	-	-		
					%	-	-	-		
成果実績及び目標値 の根拠として用いた 統計・データ名(出典) /定性的なアウトカム に関する成果実績		セキュリティバイデザインの浸透及びデジタル庁CSIRTチームの知見向上により、情報セキュリティインシデントに対する対処能力の維持・向上に努めている。								
アウトカム設定について の説明		アクティビティ①について定性的なアウトカムを設定している理由								
		庁内職員におけるセキュリティバイデザインの考え方の浸透について、その状態を表す定量的な指標が無く、定量的な指標を設定することは困難である。また、CSIRT職員については時々刻々と変化する情報セキュリティインシデント対応をめぐる環境に応じて適切な活動を行う必要があるため、現時点では定量的な成果指標を設定することが困難である。								
		アクティビティ①についてアウトカムが複数設定できない理由								
		上記の通り、定量的な目標の設定が困難であるため。								

活動内容② (アクティビティ)	デジタル庁が整備・運用するシステム(いわゆる①システム)を対象に、情報セキュリティを確保するための基本的取組として、現在制定しているセキュリティポリシー、関係規程類、政府統一基準群(令和4年度版)および関係官庁のガイドライン等各規定の準拠性を確認し、組織及び情報システムのセキュリティ確保に関する取組の実施状況について、情報セキュリティ監査を実施する。									
↓										
活動目標及び活動実績② (アウトプット)	活動目標	活動指標		単位	令和2年度	令和3年度	令和4年度	5年度 活動見込	6年度 活動見込	
	デジタル庁が整備・運用するシステム(いわゆる①システム)に対する監査の実施	監査システム数		活動実績	システム数	-	2	5	7	8
			当初見込み	システム数	-	2	3	6	7	
↓	成果目標②-1の 設定理由 (アウトプットからのつながり)									
成果目標及び成果実績②-1 (短期アウトカム)	成果目標	定量的な成果指標		単位	令和2年度	令和3年度	令和4年度	目標年度 <input type="text"/> 年度		
				成果実績	受講率	-	-	-		
				目標値	受講率	-	-	-		
			達成度	%	-	-	-	-		
↓	成果実績及び目標値の根拠として用いた統計・データ名(出典)/定性的なアウトカムに関する成果実績									
↓	成果目標②-2の 設定理由 (短期アウトカムからのつながり)									
成果目標及び成果実績②-2 (中期アウトカム)	成果目標	定量的な成果指標		単位	令和2年度	令和3年度	令和4年度	目標年度 <input type="text"/> 年度		
				成果実績						
				目標値						
			達成度	%	-	-	-	-		
↓	成果目標②-3の 設定理由 (長期アウトカムへのつながり)									
成果目標及び成果実績②-3 (長期アウトカム)	成果目標	定量的な成果指標		単位	令和2年度	令和3年度	令和4年度	目標最終年度 <input type="text"/> 年度		
	システム監査により、システム運用に際してのセキュリティ上の課題を発見・改善し、組織及び組織及び情報システムにおける情報セキュリティの確保を実現する。			成果実績	-	-	-	-	-	
				目標値	-	-	-	-	-	
			達成度	%	-	-	-	-		
アウトカム設定についての説明	アクティビティ②について定性的なアウトカムを設定している理由									
	情報セキュリティの確保については、その状態を表す定量的な指標が無く、現時点では定量的な指標を設定することは困難である。									
	アクティビティ②についてアウトカムが複数設定できない理由									
	上記の通り、定量的な目標の設定が困難であるため。									

活動内容③ (アクティビティ)		デジタル庁のシステムが使用するソフトウェアコンポーネントの構成を把握し、バックドアを含む脆弱性に対するセキュリティ対策を実施する。							
↓									
活動目標及び活動実績③ (アウトプット)		活動目標	活動指標	単位	令和2年度	令和3年度	令和4年度	5年度 活動見込	6年度 活動見込
		バックドアの検証とセキュリティ対策の実装環境整備	4年度 検証システム数	活動実績	システム数	-	-	1	
			5年度 対策の整備数	当初見込み	システム数	-	-	1	1
		6年度 対策システム数							2
↓		成果目標③-1の 設定理由 (アウトプット からのつながり)							
成果目標及び成果実績③-1 (短期アウトカム)		成果目標	定量的な成果指標	単位	令和2年度	令和3年度	令和4年度	目標年度 年度	
				成果実績	-	-	-	-	
				目標値	-	-	-	-	
				達成度	%	-	-	-	-
成果実績及び目標値の根拠として用いた統計・データ名(出典)/定性的なアウトカムに関する成果実績									
↓		成果目標③-2の 設定理由 (短期アウトカム からのつながり)							
成果目標及び成果実績③-2 (中期アウトカム)		成果目標	定量的な成果指標	単位	令和2年度	令和3年度	令和4年度	目標年度 年度	
				成果実績	-	-	-	-	
				目標値	-	-	-	-	
				達成度	%	-	-	-	-
成果実績及び目標値の根拠として用いた統計・データ名(出典)/定性的なアウトカムに関する成果実績									
↓		成果目標③-3の 設定理由 (長期アウトカム へのつながり)							
成果目標及び成果実績③-3 (長期アウトカム)		成果目標	定量的な成果指標	単位	令和2年度	令和3年度	令和4年度	目標最終年度 年度	
		デジタル庁システムのセキュリティ安全性、信頼性の確保		成果実績	-	-	-	-	
				目標値	-	-	-	-	
				達成度	%	-	-	-	-
成果実績及び目標値の根拠として用いた統計・データ名(出典)/定性的なアウトカムに関する成果実績		バックドアの検証とセキュリティ対策のための実装環境の整備を通じ、セキュリティの安全性・信頼性の確保に努めている。							
アウトカム設定についての説明		アクティビティ③について定性的なアウトカムを設定している理由							
		情報セキュリティの確保については、その状態を表す定量的な指標が無く、現時点では定量的な指標を設定することは困難である。							
		アクティビティ③についてアウトカムが複数設定できない理由							
		上記の通り、定量的な目標の設定が困難であるため。							



資金の流れ
 (資金の受け取り先が何をやっているかについて補足する)
 (単位: 百万円)

費目・用途 (「資金の流れ」においてブロックごとに最大の金額が支出されている者について記載する。費目と用途の双方で実情が分かるように記載)	A.			B.		
	費目	用途	金額 (百万円)	費目	用途	金額 (百万円)
委託料	情報セキュリティ内部監査	19.7	委託料	バックドア検証費	32.5	
計		19.7	計		32.5	
	C.			D.		
	費目	用途	金額 (百万円)	費目	用途	金額 (百万円)
委託料	セキュリティハイテクデザインの浸透を目的とした新たなセキュリティ研修の構築	19.1	参加費	CSIRT要員研修	3.8	
計		19.1	計		3.8	

費目・用途欄についてさらに記載が必要な場合はチェックの上【別紙2】に記載 チェック

支出先上位10者リスト

A.

	支出先	法人番号	業務概要	支出額 (百万円)	契約方式等	入札者数 (応募者数)	落札率	一者応札・一者応募又は競争性のない随意契約となった理由及び改善策 (支出額10億円以上)
1	株式会社バルク	4010001107293	情報セキュリティ内部監査	19.7	一般競争契約 (総合評価)	2	97.7%	

B

	支出先	法人番号	業務概要	支出額 (百万円)	契約方式等	入札者数 (応募者数)	落札率	一者応札・一者応募又は競争性のない随意契約となった理由及び改善策 (支出額10億円以上)
1	株式会社三菱総合研究所	6010001030403	バックドア検証に関する調査研究	32.5	一般競争契約 (総合評価)	2	99.9%	

C

	支出先	法人番号	業務概要	支出額 (百万円)	契約方式等	入札者数 (応募者数)	落札率	一者応札・一者応募又は競争性のない随意契約となった理由及び改善策 (支出額10億円以上)
1	NRIセキュアテクノロジーズ株式会社	8010401084443	セキュリティバイデザインの浸透を目的とした新たなセキュリティ研修の構築	191	一般競争契約 (総合評価)	2	97.7%	

D

	支出先	法人番号	業務概要	支出額 (百万円)	契約方式等	入札者数 (応募者数)	落札率	一者応札・一者応募又は競争性のない随意契約となった理由及び改善策 (支出額10億円以上)
1	株式会社サイバーディフェンス研究所	6010001120410	「AXIS サイバーセキュリティ総合」ライセンス研修の受講	0.9	随意契約(少額)	-	-	
2	株式会社ディアイティ	2010601022778	X-Ways Forensicsトレーニング(詳細解析編)研修の受講	0.9	随意契約(少額)	-	-	
3	ヒートウェーブ株式会社	9011001043111	脅威インテリジェンスセミナーの受講	0.7	随意契約(少額)	-	-	
4	株式会社Armoris	4010501044623	OSINT(Open Source Intelligence)ハンズオントレーニングの受講	0.7	随意契約(少額)	-	-	
5	株式会社サイバーディフェンス研究所	6010001120410	犯罪捜査とアクター分析のためのOSINT	0.6	随意契約(少額)	-	-	
支出先上位10者リスト欄についてさらに記載が必要な場合はチェックの上【別紙3】に記載							チェック	