事業番号　2022　－　デジ　－　21　－　0006

令和4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4年（2022年）6月7日閣議決定） サイバーセキュリティ戦略（令和3年（2021年）9月28日閣議決定）	
主要政策・施策	－			主要経費	その他の事項経費	

事業の目的（目指す姿を簡潔に。3行程度以内）	あらゆる主体がサイバー空間に参加することとなる中、サイバー空間の利用は不可欠であり、国民生活や経済活動の基盤となる重要インフラ等のサイバー攻撃によるリスクの増大から、デジタル庁が整備・運用するシステムについて、攻撃に強いシステムを企画設計する（セキュリティ・バイ・デザイン）ほか、運用・保守段階含め検証・監査等を実施し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行う環境を整備する。また、デジタル庁が整備・運用するシステムにインシデントが発生した場合には、速やかに被害の拡大を防ぎ、回復のための措置を講ずるレジリエンスを向上させたセキュリティ対応態勢を構築する。
事業概要（5行程度以内。別添可）	デジタル庁が整備・運用するシステムについて、デジタル庁セキュリティポリシーに準拠した運用管理規程が策定され、この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り組みの検証・監査・調査等を実施する。また、デジタル庁が整備・運用するシステムとともに、調達する機器・ソフトウェア等のうち重要なものの安全性を確保するため、バックドアが仕掛けられていないかの検証等を試行する。さらに、これらの検証等を踏まえ、デジタル庁のセキュリティ専門チームおよび各システム調達担当が、外部専門機関も活用しながら対策を実施できる環境を整えるため、実務的に準拠可能な整備方針・技術ガイドライン策定やセキュリティ研修等を実施する。また、インシデント発生時に、24時間365日迅速な対応を実施するための必要な環境を構築する。
実施方法	直接実施、委託・請負

予算額・執行額（単位：百万円）

		令和元年度	令和2年度	令和3年度	令和4年度	令和5年度要求
予算の状況	当初予算	－	－	－	120	125
	補正予算	－	－	－	－	
	前年度から繰越し	－	－	－	－	－
	翌年度へ繰越し	－	－	－	－	
	予備費等	－	－	138	－	
	計	0	0	138	120	125
執行額		0	0	138		
執行率（%）		－	－	100%		
当初予算＋補正予算に対する執行額の割合（%）		－	－	－		

令和4・5年度予算内訳（単位：百万円）

歳出予算目	令和4年度当初予算	令和5年度要求	主な増減理由
情報処理業務庁費	120	125	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各種研修の更なる拡充のための増額。 また、統一基準における「自己点検」や「情報セキュリティ監査」の位置付けである脆弱性診断を、デジタル庁の職員で不足無く実施することは困難であるため、外部のセキュリティ専門事業者と連携して行う新規委託費用分の増額。 「重要政策推進枠」36
計	120	125	

活動内容（アクティビティ）	デジタル庁が整備・運用するシステムとともに、調達する機器・ソフトウェア等のうち重要なものの安全性を確保するため、バックドアが仕掛けられた最新の被害事例等を調査し、デジタル庁におけるバックドア検証の定義の落とし込み、検証手法の整理及び試行を行う。また、4年度の調査結果を踏まえ、検証手順を作成し、5年度以降に、検証が必要と思われる重要なシステムから随時検証を広めることで、デジタル庁におけるセキュリティ水準の向上を随時図ることを目的とする。

活動目標及び活動実績（アウトプット）

活動目標	活動指標		単位	令和元年度	令和2年度	令和3年度	4年度活動見込	5年度活動見込
バックドア検証の実施 ※4年度は試行検証数 ※5年度は検証数	バックドア検証を実施したシステム数 ※検証範囲が情報システムになった場合を想定	活動実績	システム数	－	－	－	－	－
		当初見込み	システム数	－	－	－	1	－

単位当たりコスト

算出根拠		単位	令和元年度	令和2年度	令和3年度	4年度活動見込
※4年度はバックドア検証における事例調査（民間企業及び諸外国等）及び検証手法の検討のため記載なし	単位当たりコスト		－	－	－	－
	計算式	/	－	－	－	－

成果目標及び成果実績（アウトカム）

定量的な成果目標	成果指標		単位	令和元年度	令和2年度	令和3年度	中間目標 6 年度	目標最終年度 8 年度
8年度までにデジタル庁①システムのうち、13システムにバックドア検証を行う。	検証実施数 ※検証範囲が情報システムになった場合を想定	成果実績	システム数	－	－	－	－	－
		目標値	システム数	－	－	－	7	13
		達成度	%	1	－	－	－	－

根拠として用いた統計・データ名（出典）	－								
活動内容（アクティビティ）	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り、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のサイバー攻撃によるリスクの増大から、対策の重要性はますます大きくなっている。そのため、デジタル庁が整備・運用するシステムについて、デジタル庁セキュリティポリシーに準拠した運用管理規程が策定され、この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り組みの監査をNISCとともに実施する。								
活動目標及び活動実績（アウトプット）	活動目標	活動指標		単位	令和元年度	令和2年度	令和3年度	4年度活動見込	5年度活動見込
	デジタル庁セキュリティポリシーに対する準拠状況等の確認	監査システム数	活動実績	システム数	－	－	2	－	－
			当初見込み	システム数	－	－	2	3	－
単位当たりコスト	算出根拠			単位	令和元年度	令和2年度	令和3年度	4年度活動見込	
	※監査事業費（監査に係る一般管理費等も含む）については、計画プロセスの中で監査システム数が決まるため単位あたりコストの算出はなし		単位当たりコスト	千円	－	－	－	－	
			計算式	X/Y	－	－	－	－	
成果目標及び成果実績（アウトカム）	定量的な成果目標	成果指標		単位	令和元年度	令和2年度	令和3年度	中間目標 6 年度	目標最終年度 8 年度
	6年度までにデジタル庁①システムのうち、25システムに監査を行う ※NISC監査を含む	監査システム数	成果実績	累計システム	－	－	2	－	－
			目標値	累計システム	－	－	2	25	40
			達成度	%	－	－	100	－	－
根拠として用いた統計・データ名（出典）	－								
活動内容（アクティビティ）	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検証・監査を実施することとし、その実施体制をデジタル庁とIPAが共同して構築し、令和4年度（2022 年度）以降、デジタル庁①システムを中心に、デジタル庁に設置するセキュリティの専門のチーム及びデジタル庁の依頼に応じて IPA が、整備・運用等の段階において整備方針等に沿っているか等を継続的に確認する。								
活動目標及び活動実績（アウトプット）	活動目標	活動指標		単位	令和元年度	令和2年度	令和3年度	4年度活動見込	5年度活動見込
	システム監査の実施 ※4年度はシステム監査試行数 ※5年度はシステム監査数	監査試行及び監査したシステム数	活動実績	システム数	－	－	－	－	－
			当初見込み	システム数	－	－	－	2	－
単位当たりコスト	算出根拠			単位	令和元年度	令和2年度	令和3年度	4年度活動見込	
	※4年度はシステム監査における事例調査及び監査手法の検討のため、単位あたりコストはなし （本監査ではない試行実施のため記載なし）		単位当たりコスト		－	－	－	－	
			計算式	/	－	－	－	－	
成果目標及び成果実績（アウトカム）	定量的な成果目標	成果指標		単位	令和元年度	令和2年度	令和3年度	中間目標 6 年度	目標最終年度 8 年度
	デジタル庁①システムのうち、毎年度2システムにシステム監査を実施し、令和8年度までに計8システムのシステム監査完了を目指す。	システム監査したシステム数	成果実績	システム数	－	－	－	－	－
			目標値	システム数	－	－	－	4	8
			達成度	%	－	－	－	－	－
根拠として用いた統計・データ名（出典）	－								
活動内容（アクティビティ）	サイバーセキュリティ対策については、全ての政府機関等において共通的に必要とされるセキュリティ対策である統一基準群を前提のものとして引き続き実施、推進しつつ、デジタル庁の整備・運用する情報システムのセキュリティ対策については、整備方針に従って整備を進めるとともに、NISC とも連携してこれらを実践するための参考となる技術ガイドライン等を策定する。加えて、技術ガイドライン等の普及・浸透等のために必要な研修・勉強会の開催や、技術ガイドラインの実装等のために必要な機器等の調達を行う。								
活動目標及び活動実績（アウトプット）	活動目標	活動指標		単位	令和元年度	令和2年度	令和3年度	4年度活動見込	5年度活動見込
	セキュリティ対策を実践するため、参考となる技術ガイドラインを策定する。	策定した技術ガイドライン数	活動実績	件	－	－	－	－	－
			当初見込み	件	－	－	－	5	－
単位当たりコスト	算出根拠			単位	令和元年度	令和2年度	令和3年度	4年度活動見込	
	X＝年度執行額（円） ／　Y＝技術ガイドライン策定数		単位当たりコスト	円	－	－	－	7,837,400	
			計算式	X / Y	－	－	－	39,187,000/5	

定量的な成果目標の設定が困難な場合											
	定量的な目標が設定できない理由及び定性的な成果目標	定量的な目標が設定できない理由					定性的な成果目標と令和元年～令和3年度の達成状況・実績				
		右記の目標にどの程度貢献したかを寄与率を算出できないため数値化することは困難であることから、定量的な成果目標を設定することができない。					デジタル庁が整備・運用するシステムのサイバーセキュリティの確保				
	事業の妥当性を検証するための代替的な達成目標及び実績	代替目標	代替指標		単位	令和元年度	令和2年度	令和3年度	中間目標 6 年度	目標最終年度 8 年度	
		セキュリティ対策を実践するため、参考となる技術ガイドライン等の策定によるセキュリティ対策の高度化。	セキュリティ対策に関する技術ガイドライン等の策定数	実績	件	－	－	－	－	－	
				目標値	件	－	－	－	10	15	
				達成度	%	－	－	－	－	－	
	活動内容（アクティビティ）	インシデントが発生した場合には、セキュリティ専門チームの知見を生かしながら、速やかに被害の拡大を防ぎ、回復のための措置を講ずるレジリエンスを向上させたセキュリティ対応態勢が重要となる。デジタル庁に関わる情報セキュリティインシデント発生時の対処の一元管理及び情報セキュリティインシデントへの迅速かつ的確な対処をおこないサイバーセキュリティを確保する。									
	活動目標及び活動実績（アウトプット）	活動目標	活動指標		単位	令和元年度	令和2年度	令和3年度	4年度 活動見込	5年度 活動見込	
		情報セキュリティインシデントに関する情報の集約及び発生時の適切な対処・回復によるデジタル庁が整備・運用するシステムのサイバーセキュリティの確保	24時間365日迅速な対応	活動実績	日	－	－	211	－	－	
				当初見込み	日	－	－	211	365	－	
	単位当たりコスト	算出根拠			単位	令和元年度	令和2年度	令和3年度	4年度活動見込		
		X＝年度執行額（円） ／　Y＝活動日数（日）		単位当たりコスト	円	－	－	119,749	－		
				計算式	X / Y	－	－	25,267,000/211	－		
	成果目標及び成果実績（アウトカム）	定量的な成果目標	成果指標		単位	令和元年度	令和2年度	令和3年度	中間目標 － 年度	目標最終年度 － 年度	
		－	－	成果実績	－	－	－	－	－	－	
				目標値	－	－	－	－	－	－	
				達成度	%	－	－	－	－	－	
	根拠として用いた統計・データ名（出典）	－									
定量的な成果目標の設定が困難な場合											
	定量的な目標が設定できない理由及び定性的な成果目標	定量的な目標が設定できない理由					定性的な成果目標と令和元年～令和3年度の達成状況・実績				
		右記の目標にどの程度貢献したかを寄与率を算出できないため数値化することは困難であることから、定量的な成果目標を設定することができない。					デジタル庁が整備・運用するシステムのサイバーセキュリティの確保				
	事業の妥当性を検証するための代替的な達成目標及び実績	代替目標	代替指標		単位	令和元年度	令和2年度	令和3年度	中間目標 － 年度	目標最終年度 － 年度	
		サイバーセキュリティに関する事象の発生及び被害の防止を図る。	情報セキュリティに関する重大なインシデントの発生件数	実績	－	－	－	0	－	－	
				目標値	－	－	－	0	－	－	
				達成度	%	－	－	－	－	－	

成果目標及び成果実績（アウトカム）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1】に記載	チェック	

事業所管部局による点検・改善

	項　目	評 価	評価に関する説明
国費投入の必要性	事業の目的は国民や社会のニーズを的確に反映しているか。	○	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り、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のサイバー攻撃によるリスクの増大から、対策の重要性は大きくなっている。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、誰一人取り残されないサイバーセキュリティの確保が求められている。
	地方自治体、民間等に委ねることができない事業なのか。	○	利便性の向上の徹底と国民への行政サービス等を安定して安全に提供するといった観点を含めたサイバーセキュリティの確保の両立が不可欠であることから、サイバーセキュリティ戦略・統一基準群に基づき、デジタル庁で進めるべき事業である。
	政策目的の達成手段として必要かつ適切な事業か。政策体系の中で優先度の高い事業か。	○	デジタル社会の実現に向けた重点計画の政策目的を達成するためには、必要不可欠な事業である。また、近年、サイバー空間を取り巻く状況は高度化・複雑化するとともに、技術の進歩等により急速な拡張・発展を遂げている。このような状況の中、デジタル社会の実現に関する司令塔として、デジタル庁の役割は増大しており、国民が安心して参加できるデジタル社会の実現を図るためには、本業務の優先度は高いと考えられる。
事業の効率性	競争性が確保されているなど支出先の選定は妥当か。	○	企画競争、一般競争入札で調達を行ったものについては複数の事業者より応札がされており競争性が確保されている。競争性のない随意契約で調達を行ったものについては、デジタル社会の実現に向けた重点計画を実施するためなど、随意契約を行ったものである。
	一般競争契約、指名競争契約又は随意契約（企画競争）による支出のうち、一者応札又は一者応募となったものはないか。	有	
	競争性のない随意契約となったものはないか。	有	
	受益者との負担関係は妥当であるか。	-	―
	単位当たりコスト等の水準は妥当か。	○	事業を計画するに当たっては、可能な限り、事前に複数の業者の見積もりを取得するなど、適正なコスト水準になるように努めている。
	資金の流れの中間段階での支出は合理的なものとなっているか。	-	―
	費目・使途が事業目的に即し真に必要なものに限定されているか。	○	費目・使途は、この事業目的に即して真に必要なものに限定されている。
	不用率が大きい場合、その理由は妥当か。（理由を右に記載）	-	―
	繰越額が大きい場合、その理由は妥当か。（理由を右に記載）	-	―
	その他コスト削減や効率化に向けた工夫は行われているか。	○	調達内容の見直しによりコスト削減に務めるとともに、公示期間の十分な確保等によって競争性を確保している。
事業の有効性	成果実績は成果目標に見合ったものとなっているか。	-	―
	事業実施に当たって他の手段・方法等が考えられる場合、それと比較してより効果的あるいは低コストで実施できているか。	-	―
	活動実績は見込みに見合ったものであるか。	-	―
	整備された施設や成果物は十分に活用されているか。	-	
関連事業	関連する事業がある場合、他部局・他府省等と適切な役割分担を行っているか。（役割分担の具体的な内容を各事業の右に記載）	-	

事業番号					事業名

点検・改善結果		
	点検結果	真に必要な業務に対する執行、成果物の有効活用等に努めている。
	改善の方向性	早期執行に努めることで、今以上に契約準備、市場価格調査、入札公告等の期間の確保を図ることにより、適切な業務実施に努めたい。

外部有識者の所見
・バックドア検証に関して検証を実施したシステム数を指標とすることは適切だが、一方で検証はシステムの規模や複雑性に大きく依存することから、システムの規模や複雑性についても明記すべきである。 ・行政システムのセキュリティはNISCの取り組みと重なるところがある。デジタル庁のセキュリティ対策の中で、NISCにおける活動と重なる部分に関しては、NISCの指標を取り入れるなどして、政府内の指標との整合性をもたせるべきである。 ・セキュリティ組織やプロセス、システム上のサイバーセキュリティ対策は最重要課題であり、国費投入の必要性や優先度も高いと理解している。最重要課題でありながら、事業の効率性、並びに有効性に関する評価や説明の記述が簡易であり、十分な評価説明が必要である。評価としては、データ、個人情報等の管理、適切なICT投資、ガバナンス、リテラシーやリスクアセスメント評価等も一考である。 ・IPAをはじめとして、他の機関との重複コストにならないよう情報共有を行い、連携していくことも必要。 ・テレワークや遠隔教育など、サイバー空間での活動が急激に増えている我が国で、サイバー空間の安全性が保たれることは必須の要件である。 ・国の安全性をサイバー空間の安全性の議論抜きには語れないことは、ロシアによるウクライナへの軍事侵攻においても明らかである。サイバーセキュリティ向上のための本政策は、積極的に取り組むべきである。

行政事業レビュー推進チームの所見	
現状通り	外部有識者の所見を踏まえて、検討すること。

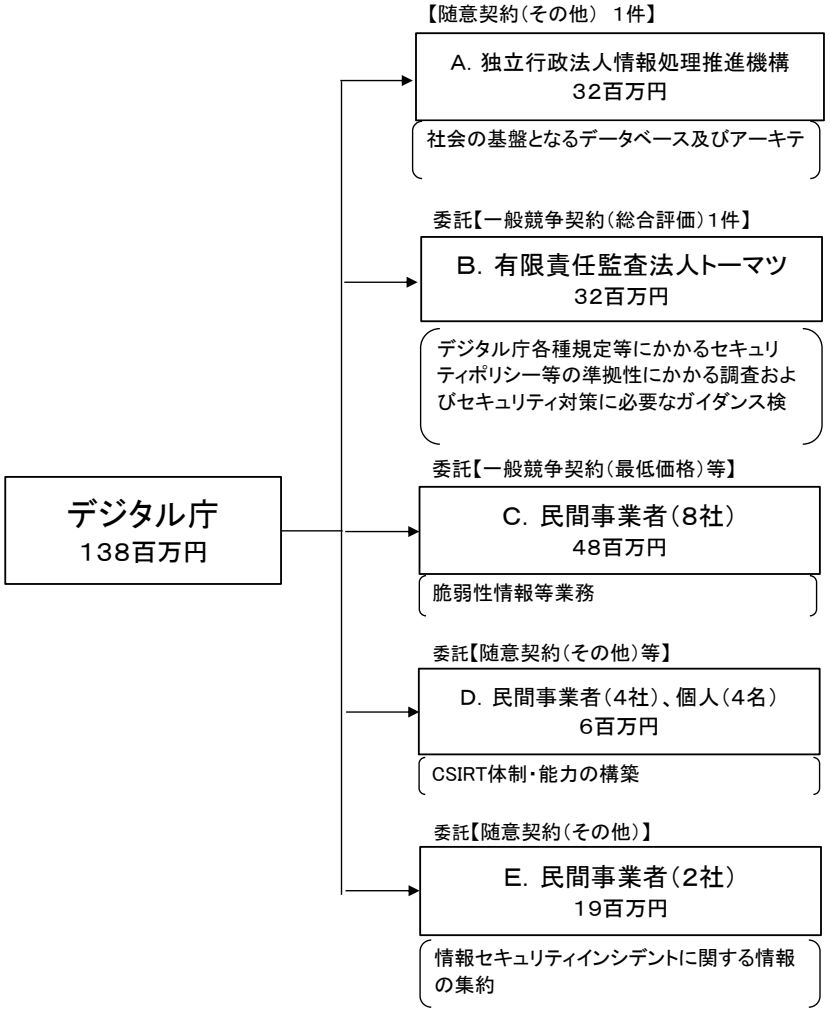
所見を踏まえた改善点/概算要求における反映状況	
現状通り	いただいた所見を踏まえ、レビューシートに追記を行うとともに、ご指摘いただいた事業の重要性を踏まえ、引き続き事業の有効性・効率性・成果について適切かつ的確に検証し、予算の効率的執行に努める。

備考

関連する過去のレビューシートの事業番号				
平成23年度				
平成24年度				
平成25年度				
平成26年度				
平成27年度				
平成28年度				
平成29年度				
平成30年度				
令和元年度				
令和2年度				
令和3年度				

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

※令和3年度実績を記入。執行実績がない新規事業、新規要求事業については現時点で予定やイメージを記入。



費目・使途
（「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。費目と使途の双方で実情が分かるように記載）

A.独立行政法人情報処理推進機構

費目	使途	金額（百万円）
人件費	社会の基盤となるデータベース及びアーキテクチャの検討にかかる調査研究	32
計		32

B.有限責任監査法人トーマツ

費目	使途	金額（百万円）
人件費	デジタル庁各種規定等にかかるセキュリティポリシー等の準拠性にかかる調査およびセキュリティ対策に必要なガイダンス検討等にかかる調査研究	32
計		32

C.AOSデータ株式会社

費目	使途	金額（百万円）
備品費	脆弱性情報等業務	39
計		39

D.NRIセキュアテクノロジーズ株式会社

費目	使途	金額（百万円）
参加費	受講料	2.7
計		2.7

E.y株式会社

費目	使途	金額（百万円）
運用経費	情報セキュリティインシデントに関する情報の集約に係る経費	15
計		15

F.

費目	使途	金額（百万円）
計		0

費目・使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	独立行政法人情報処理推進機構	5010005007126	社会の基盤となるデータベース及びアーキテクチャの検討にかかる調査	32	随意契約（その他）	1	100%	-

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	有限責任監査法人トーマツ	5010405001703	デジタル庁各種規定等にかかるセキュリティポリシー等の準拠性にかかる調査およびセキュリティ対策に必要なガイダンス検討等にかかる調査研究	32	一般競争契約（総合評価）	1	59.7%	-

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	.AOSデータ株式会社	8010401117533	サイバー攻撃対処・分析システムの整備	36.7	一般競争契約（最低価格）	3	88.3%	-
2	.AOSデータ株式会社	8010401117533	脆弱性検査ソフトウェア利用者アカウントの追加	1.8	一般競争契約（最低価格）	1	68%	-
3	株式会社バルク	4010001107293	脆弱性診断支援役務	4.1	一般競争契約（最低価格）	1	59.1%	-
4	株式会社バルク	4010001107293	脆弱性診断支援役務	1.1	一般競争契約（最低価格）	2	71%	-
5	テガラ株式会社	3080401003319	脅威情報提供サービスの購入	1	随意契約（その他）	-	100%	-
6	株式会社サードウェーブ	4010001018053	脆弱性情報及び検査記録保存用記憶媒体の取得	0.9	随意契約（少額）	-	-	-
7	日本コムシス株式会社	4010701022825	サイバー攻撃対処・分析システムの先行配備	0.9	随意契約（少額）	-	-	-
8	ムードゥーセキュリティ株式会社	8020001104402	フォレンジック訓練用資機材	0.8	随意契約（少額）	-	-	-
9	株式会社ブロード・アクセス	9010601041227	脆弱性診断及びインシデント対応用ネットワーク回線の延長	0.8	随意契約（少額）	-	-	-
10	株式会社朝日ネット	9010001035779	ASAHINET光クロス	0.1	随意契約（少額）	-	-	-

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	NRIセキュアテクノロジーズ株式会社	8010401084443	Windowsフォレンジック研修への参加	1.9	随意契約（その他）	－	100%	－
2	エヌ・ティ・ティ・コミュニケーションズ株式会社	7010001064648	情報セキュリティ対策に資する支援役務	1.4	一般競争契約（最低価格）	2	60.8%	－
3	グローバルセキュリティエキスパート株式会社	2010401086255	CEH研修への参加	1	随意契約（少額）	－	－	－
4	株式会社ディアイティ	2010601022778	X－Waysフォレンジックストレーニング（初級）研修への参加	0.9	随意契約（少額）	－	－	－
5	NRIセキュアテクノロジーズ株式会社	8010401084443	クラウドフォレンジックの研修への参加	0.8	随意契約（少額）	－	－	－
6	個人A	－	CYDER－C研修への参加	0.1	その他	－	－	－
7	個人B	－	CYDER－C研修への参加	0.1	その他	－	－	－
8	個人C	－	CYDER－C研修への参加	0.1	その他	－	－	－
9	個人D	－	CYDER－C研修への参加	0.1	その他	－	－	－

E

	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	y株式会社	－	インシデント対応のための調査	15	随意契約（その他）	－	100%	－
2	z株式会社	－	インシデント対応のための調査	3.9	随意契約（その他）	－	100%	－