

政策評価調書（個別票1）

【政策ごとの予算額等】

政策名		安心できるIT社会の実現				
評価方式		実績評価	政策目標の達成度合い	相当程度進展あり	番号	⑦
		25年度	26年度	27年度	28年度	29年度概算要求額
予算 の 状 況	当初予算（千円）	239,395 <104,147,348>	220,474 <110,563,330>	229,703 <116,796,012>	185,282 <125,096,438>	184,176 <130,769,872>
	補正予算（千円）	142,945 <12,706,990>	85,473 <12,116,438>	0 <9,773,369>		
	繰越し等（千円）	175,800 <42,746,493>	0 <10,179,006>	0 <10,583,225>		
	計（千円）	558,140 <159,600,831>	305,947 <132,858,774>	229,703 <137,152,606>		
	執行額（千円）	484,880 <139,208,144>	253,320 <116,241,880>	206,755 <120,909,112>		
政策評価結果の概算要求への反映状況		既存の施策を引き続き推進すべきであるとされた政策評価結果を踏まえ、サイバーセキュリティの確保とサイバー犯罪・サイバー攻撃の抑止に必要な経費を概算要求した。				

政策評価調書（個別票2）

【政策に含まれる事項の整理】

政策名	安心できるIT社会の実現					番号	⑦		(千円)
	予 算 科 目						予 算 額		
整理番号	会計	組織／勘定	項	事項	28年度当初予算額	29年度概算要求額			
対応表において●となっているもの	●	1	一般	警察庁	情報技術犯罪対策費	情報技術犯罪対策に必要な経費	185,282	184,176	-1,196
	●	2	一般	警察庁	科学警察研究所	研究・鑑定等に必要な経費	< 810,664 >	< 1,010,448 >	
	●	3	一般	警察庁	警察活動基盤整備費	警察活動基盤の整備に必要な経費	< 122,975,439 >	< 128,806,718 >	
	●	4	東日本大震災復興特別	警察庁	治安復興事業費	警察活動基盤の整備に必要な経費	< 570,813 >	< 341,795 >	
	●	5	東日本大震災復興特別	警察庁	治安復興政策費	警察活動基盤の整備に必要な経費	< 739,522 >	< 610,911 >	
	小計						185,282	184,176	-1,196
						<125,096,438> の内数	<130,769,872> の内数		
対応表において◆となっているもの									
	小計								
対応表において○となっているもの						< >	< >		
						< >	< >		
						< >	< >		
						< >	< >		
	小計						の内数	の内数	
対応表において◇となっているもの						< >	< >		
						< >	< >		
						< >	< >		
						< >	< >		
	小計						の内数	の内数	
合計						185,282	184,176	-1,196	
						<125,096,438> の内数	<130,769,872> の内数		

政策評価調書（個別票3）

【見直しの内訳・具体的な反映内容】

政策名		安心できるIT社会の実現				番号	⑦	(千円)
事務事業名	整理番号		予算額			政策評価結果の反映による見直し額(削減額)	政策評価結果の概算要求への反映内容	
			28年度当初予算額	29年度概算要求額	増減			
アクセス制御機能に関する技術の研究開発の状況等に関する調査及び広報啓発等	●	1	8,617	7,421	△ 1,196	△ 1,196	既存の施策を引き続き推進すべきであるとされた政策評価結果を踏まえ、アクセス制御機能に関する技術の研究開発の状況等に関する調査及び広報啓発等に必要な予算を要求する一方、執行状況に基づいた見直しを行い、経費の削減を図った。	
合計			8,617	7,421	△ 1,196	△ 1,196		

平成28年度実績評価計画書(政策評価の事前分析表)

基本目標7 業績目標1

基本目標	安心できるIT社会の実現	政策所管課	総務課、情報技術犯罪対策課、警備企画課、情報技術解析課	政策評価実施予定時期	29年7月頃							
業績目標	サイバーセキュリティの確保とサイバー犯罪・サイバー攻撃の抑止	政策体系上の位置付け	安心できるIT社会の実現									
業績目標の説明	ITが国民生活や社会経済活動に多大な影響を与える存在となっていることを踏まえ、サイバー空間をめぐる脅威に対処するとともに、サイバー犯罪の取締り、サイバー攻撃対策等を総合的に進めることにより、安心できるIT社会を実現する。											
業績指標	達成目標	基準年	達成年	年(年度)ごとの実績値・施策の推進状況(実績)								目標設定の考え方及び根拠
				項目	23年	24年	25年	26年	27年	25~27年(平均)	28年	
① サイバー犯罪対策に係る取組状況(事例)	サイバー関連事業者等との連携強化等により、サイバー犯罪対策を推進する。		28年度									サイバー関連事業者等との連携強化等の推進状況は、サイバー犯罪の抑止の度合いを測る一つの指標となるため。
② サイバー攻撃対策に係る取組状況(事例)	関係機関、サイバー攻撃の標的となるおそれのある国内の事業者等との連携強化等により、サイバー攻撃対策を推進する。		28年度									関係機関、サイバー攻撃の標的となるおそれのある国内の事業者との連携強化等の推進状況は、サイバー攻撃による被害の未然防止・拡大防止等の度合いを測る一つの指標となるため。
参考指標	項目	年ごとの実績値							参考指標の考え方			
		23年	24年	25年	26年	27年	23~27年(平均)	28年				
① サイバー犯罪(注1)の検挙件数	合計(件)	5,741	7,334	8,113	7,905	8,096	7,438		サイバー犯罪の検挙件数は、サイバー犯罪の抑止の度合いを測る一つの指標となる。			
	不正アクセス行為の禁止等に関する法律違反	248	543	980	364	373	502					
	コンピュータ・電磁的記録対象犯罪及び不正指令電磁的記録に関する罪	105	178	478	192	240	239					
	ネットワーク利用犯罪	5,388	6,613	6,655	7,349	7,483	6,698					
② サイバー犯罪等に関する相談受理件数	合計(件)	80,273	77,815	84,863	118,100	128,097	97,830		サイバー犯罪等に関する相談受理件数は、サイバー犯罪の抑止の度合いを測る一つの指標となる。			
	詐欺・悪質商法	32,892	29,113	36,237	58,340	67,026	44,722					
	迷惑メール	11,667	12,946	10,682	14,185	16,634	13,223					
	名誉毀損・誹謗中傷	10,549	10,807	9,425	9,757	10,398	10,187					
	インターネット・オークション	5,905	4,848	5,950	6,545	6,274	5,904					
	不正アクセス・ウイルス	4,619	4,803	6,220	9,550	7,089	6,456					
	違法情報・有害情報	3,382	3,199	3,132	5,080	4,854	3,929					
	その他	11,259	12,099	13,217	14,643	15,822	13,408					

③ インターネットバンキングに係る不正送金事犯の発生件数及び被害額	発生件数(件)	165	64	1,315	1,876	1,495	983		インターネットバンキングに係る不正送金事犯の発生件数及び被害額は、サイバー犯罪の抑止の度合いを測る一つの指標となる。
	被害額(万円)	30,800	4,800	140,600	291,000	307,300	154,900		
④ インターネット・ホットラインセンターが受理した違法情報件数	違法情報(件) (注2)	36,573	38,933	30,371	35,013	72,073	42,593		インターネット・ホットラインセンターが受理した違法情報の件数は、インターネット上における違法情報の流通に対する抑止の度合いを測る一つの指標となる。
⑤ 出会い系サイト及びコミュニティサイトの利用に起因する犯罪に遭った児童の数	出会い系サイトの利用に起因する犯罪被害に遭った児童数(人)	282	218	159	152	93	181		出会い系サイト及びコミュニティサイトの利用に起因する犯罪に遭った児童の数は、出会い系サイト及びコミュニティサイトに関する児童被害の防止に向けた対策の推進の度合いを測る一つの指標となる。
	コミュニティサイトの利用に起因する犯罪被害に遭った児童数(人)	1,085	1,076	1,293	1,421	1,652	1,305		
⑥ 標的型メール攻撃の把握件数	標的型メール攻撃の把握件数(件)		1,009	492	1,723	3,828	1,763		「サイバーインテリジェンス情報共有ネットワーク」(注3)を通じて警察が把握した標的型メール攻撃の件数は、サイバー攻撃をめぐる情勢を把握する際の一つの指標となる。
⑦ サイバーテロ(注4)の発生件数	発生件数(件)	0	0	0	0	0	0		サイバーテロの発生件数は、IT社会におけるサイバーセキュリティの確保の度合いを測る一つの指標となる。

注1 高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪
注2 児童ポルノ画像、わいせつ画像、覚醒剤等規制薬物の広告に関する情報等、インターネット上に掲載すること自体が違法となる情報
注3 23年8月、標的型メール攻撃に関する情報を共有することで被害拡大の防止を図ることを目的として、警察と先端技術を有する事業者等が構築した情報共有ネットワークで、28年1月現在、7,333社が参画している。
注4 重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いもの

達成手段 (開始年度)	補正後予算額(執行額)		28年度 概算要求額	関連する 業績指標	達成手段の概要等	28年行政事業レビュー	
	26年度	27年度				事業番号	事業名
(1) 全国協働捜査方式の推進、捜査官の育成、各種資機材の整備等によるサイバー犯罪対策の体制の強化				①・参①・参③	効率的な捜査活動を推進するための全国協働捜査方式を推進するとともに、サイバー犯罪対策に従事する警察職員に対し、サイバー犯罪に関する専門知識を習得させるための研修を実施するほか、サイバー犯罪捜査や解析のために必要な資機材を整備するなどして、適正なサイバー犯罪捜査を推進するとともに、サイバー犯罪の抑止を図る。	62	サイバー犯罪取締りの推進
(2) 警察職員への研修等によるサイバー攻撃対策のための体制強化(13年度)				②・参⑦	サイバー攻撃対策に従事する警察職員に対し、サイバー攻撃手法等に関する研修及び民間委託による訓練等を実施するほか、新たなサイバー攻撃に対応できる資機材を整備するなどし、サイバー攻撃の発生及び被害の拡大の防止を図る。	65	サイバー攻撃対策の推進
(3) 予防・捜査等の推進に必要なインターネット観測の推進				②・参⑦	リアルタイム検知ネットワークシステムを運用しサイバー攻撃の予兆・実態把握に努めるとともに、同システムの高度化に資するインターネット観測技術に関する調査研究を実施し、サイバーテロの発生及び被害の拡大の防止を図る。		
(4) 情勢に対応した訓練環境の充実				①・②・参①・参⑦	各種サイバー犯罪事案やサイバー攻撃事案を疑似的に体験できる訓練環境を充実させるとともに、全国警察のサイバー犯罪対策やサイバー攻撃対策を担当する職員等に対して実践的な訓練を実施するなどし、サイバー犯罪の抑止並びにサイバーテロの発生及び被害の拡大の防止を図る。	63	情勢に対応した訓練環境の充実
(5) 各種講演やセミナーによる研修及びウェブサイト等を活用した情報発信を通じた情報セキュリティ対策に関する広報啓発				①・参①・参③	警察やプロバイダ連絡協議会等が主催する研修会、学校等における講演会、情報通信技術関連イベント等における講演やセミナーを実施するほか、警察庁ウェブサイトのサイバー犯罪対策のサイトやセキュリティポータルサイト(@police)、情報セキュリティ対策DVD、広報啓発用リーフレット等を活用して、情報セキュリティに関する広報啓発を行い、積極的な通報を喚起するなどし、サイバー犯罪の抑止を図る。	61	アクセス制御機能に関する技術の研究開発の状況等に関する調査及び広報啓発等
(6) サイバーテロ対策協議会、共同訓練等の実施による重要インフラ事業者等との連携				②・参⑦	事業者等への個別訪問、サイバーテロ対策協議会等を通じた情報セキュリティに関する情報提供、事案発生を想定した共同訓練、意見交換等により、サイバー攻撃の標的となるおそれのある国内の事業者等との連携強化並びにサイバーテロの発生及び被害の拡大の防止を図る。		
(7) 情報窃取の標的となるおそれのある事業者等との連携				②・参⑥	サイバー攻撃に関する情報を集約・分析し、その結果を事業者等と共有することで、サイバー攻撃の標的となるおそれのある国内の事業者等との連携強化並びにサイバーインテリジェンスの発生及び被害の拡大の防止を図る。		
(8) 国際捜査協力及び情報セキュリティに関する情報共有等によるサイバー犯罪取締り等のための国際連携の強化				①・②・参①・参③・参⑦	G8ハイレベル犯罪サブグループ会合への出席、アジア大洋州地域サイバー犯罪捜査技術会議の開催、国際刑事警察機構(ICPO-Interpol)を通じたサイバー犯罪・サイバー攻撃事案に係る国際捜査共助の実施により、犯罪取締り等のための諸外国との国際連携を強化し、サイバー犯罪の抑止並びにサイバーテロの発生及び被害の拡大の防止を図る。		

(9)	先進的なサイバー犯罪に対応するための効果的な抑止・捜査手法の活用	参①・参③	ファイル共有ソフトを悪用した著作権侵害事犯について一斉取締りを行うなど効果的な取締りを実施するほか、システムの運用により、各都道府県警察において個別に把握したサイバー犯罪に関する捜査情報等の共有を図るなど、合同・共同捜査を積極的に推進して効率的な捜査活動を行い、サイバー犯罪の抑止を図る。	62	サイバー犯罪取締りの推進
(10)	情報技術解析に係る関係機関との連携強化	①・②・参①・参③・参⑦	情報技術の解析に係る国内外の関係機関、民間有識者等との情報共有を行い、サイバー犯罪の抑止並びにサイバーテロの発生及び被害の拡大の防止を図る。		
(11)	総合セキュリティ対策会議の開催等による産業界等との連携強化	①・参①・参③	総合セキュリティ対策会議の開催や、不正アクセス防止対策に関する官民意見集約委員会(官民ボード)の運営を行うほか、プロバイダ連絡協議会等においてサイバー犯罪情勢や対策の在り方等について検討や情報交換を行うとともに、インターネットに係る最新の技術に関する情報及び電子機器等の解析に必要な技術情報を得るため、民間企業との技術協力を推進するなどし、サイバー犯罪の抑止を図る。	61 62	アクセス制御機能に関する技術の研究開発の状況等に関する調査及び広報啓発等 サイバー犯罪取締りの推進
(12)	インターネット・ホットライン業務(注5)の効果的運用(18年度)	参①・参④	警察庁が業務委託しているインターネット・ホットラインセンターにおいて、一般のインターネット利用者等から違法情報等に関する通報を受理し、サイト管理者等への削除依頼、警察への通報等を行うことにより、各都道府県警察において効率的かつ効果的な取締りを推進し、サイバー犯罪の抑止を図る。	59	インターネット・ホットライン業務
(13)	インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律の効果的な運用(15年度)	参①・参⑤	インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律の効果的な運用により、サイバー犯罪の抑止を図る。		
(14)	サイバー防犯ボランティアの育成・支援	参①・参④	サイバー防犯ボランティアの育成・拡充を促進して、サイバー空間の規範意識の向上や安全・安心に対する国民の意識を醸成するほか、団体数の増加などで活動の活性化を図ることによって、サイバー犯罪の抑止を図る。	59	インターネット・ホットライン業務
注5 一般のインターネット利用者等からインターネット上の違法情報(児童ポルノ画像、わいせつ画像、覚醒剤等規制薬物の広告に関する情報等、インターネット上に掲載すること自体が違法となる情報)等に係る通報を受け付け、警察に通報したり、サイト管理者等に削除依頼を実施する業務					
基本目標に係る予算額等		基本目標に係る予算額等は、26年度執行額253,320千円(116,241,880千円)、27年度当初予算額229,703千円(116,796,012千円)、28年度政府予算案185,282千円(125,096,438千円)であった(情報技術犯罪対策費、〈〉内は複数の政策にわたる経費)。			
業績目標に係る内閣の重要政策(施政方針演説等のうち主なもの)		<ul style="list-style-type: none"> ○ 「『世界一安全な日本』創造戦略」(25年12月10日閣議決定) Ⅲ 戦略の内容 <ul style="list-style-type: none"> 1 世界最高水準の安全なサイバー空間の構築 ○ サイバーセキュリティ戦略(27年9月4日閣議決定) 5 目的達成のための施策 <ul style="list-style-type: none"> 2 国民が安全で安心して暮らせる社会の実現 3 国際社会の平和・安定及び我が国の安全保障 			

平成27年度実績評価書

基本目標7 業績目標1

基本目標	安心できるIT社会の実現					
業績目標	情報セキュリティの確保とネットワーク利用犯罪等サイバー犯罪の抑止					
業績目標の説明	ITが国民生活や社会経済活動に多大な影響を与える存在となっていることを踏まえ、情報セキュリティを確保するとともに、ネットワーク利用犯罪を始めとするサイバー犯罪の取締り、サイバー攻撃対策を進めることにより、安心できるIT社会を実現する。					
基本目標に関する 予算額・執行額	区分	25年度	26年度	27年度	28年度	
	予算の 状況 (千円)	当初予算(a)	239,395 <104,147,348>	220,474 <110,563,330>	229,703 <116,796,012>	185,282 <125,096,438>
		補正予算(b)	142,945 <12,706,990>	85,473 <12,116,438>	0 <9,773,369>	
		繰越し等(c)	175,800 <42,746,493>	0 <10,179,006>		
		合計(a+b+c)	558,140 <159,600,831>	305,947 <132,858,774>		
執行額(千円)	484,880 <139,208,144>	253,320 <116,241,880>				
※ 上段には情報技術犯罪対策費を、下段には複数の基本目標に係る共通経費を、それぞれ計上した。						
業績目標に関する内閣 の重要政策(施政方針演 説等のうち主なもの)	○ 「「世界一安全な日本」創造戦略」(25年12月10日閣議決定) Ⅲ 戦略の内容 1 世界最高水準の安全なサイバー空間の構築					
	○ 「世界最先端IT国家創造宣言」(27年6月30日全部変更) Ⅳ. 利活用の裾野拡大を推進するための基盤の強化 3. サイバーセキュリティ					
	○ 「サイバーセキュリティ戦略」(27年9月4日閣議決定) 5.2 国民が安全で安心して暮らせる社会の実現 5.3 国際社会の平和・安定及び我が国の安全保障					
	○ 第190回国会における安倍内閣総理大臣施政方針演説(28年1月) 二 地方創生への挑戦					

業績指標①	項目	基準						実績
		22年	23年	24年	25年	26年	24~26年 (平均)	27年
サイバー犯罪(注 1)の検挙件数	検挙件数(件)	6,933	5,741	7,334	8,113	7,905	7,784	8,096
	(28年4月情報技術犯罪対策課作成)							
注1: 高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪								
達成状況: ○	達成目標	サイバー犯罪の検挙件数を過去3年間の平均値よりも増加させる。						
業績指標②	実績							
情報セキュリティ関 連事業者等との連 携状況(事例)	【事例1】 27年4月、警視庁において、インターネットバンキングに係る不正送金を自動で行うといった機能を有する不正プログラムに国内外の約8万2,000台の端末が感染していることを把握し、プロバイダを通じた国内の感染端末の利用者に対する注意喚起等を行った。							
	【事例2】 27年11月、一般財団法人日本サイバー犯罪対策センターの協力を得て、18都道府県警察において海外サーバ利用の違法アダルトアフィリエイト(宣伝広告)サイトの一斉取締りを行った。							
達成状況: ◎	達成目標	情報セキュリティ関連事業者等との連携を強化する。						

業績指標③	実績							
サイバー攻撃の標的となるおそれのある国内の事業者等との連携状況(事例)	【事例1】27年11月、三重県警察では、伊勢志摩サミットを見据えたサイバー攻撃対策の一環として、重要インフラ事業者等の職員を対象としたサイバー攻撃対策セミナーを実施した。セミナーにおいては、民間の有識者による講演を実施し、サイバー攻撃に関する最近の情勢及び対策について受講者の理解の醸成を図った。また、サイバー攻撃を受けたことを想定した事案対処に関する演習を、実際にパソコンを使用して実施することにより、受講者の緊急時の対処能力の向上を図った。							
	【事例2】27年10月、千葉県警察では、神奈川県警察と連携し、鉄道事業者の基幹システムが標的型メールによるサイバー攻撃を受けたとの想定で、事業者との共同対処訓練を実施した。訓練の実施に当たっては、民間の有識者の助言を受けて作成した想定シナリオを使用したほか、あらかじめ構築した同事業者の基幹システムの模擬ネットワークを使用し、実際にサイバー攻撃が発生した場合と同様の対処を行うなど、より実践的な内容とすることで、事案対処能力の更なる向上を図った。							
	上記事例のほか、国内の事業者等との連携に際しては、サイバー攻撃情勢に応じて訓練内容や事業者に対するセミナー内容の見直しを図りながら継続して実施している。27年度中もサイバー攻撃情勢を踏まえた的確な連携を実施した。							
達成状況:◎	達成目標	サイバー攻撃の標的となるおそれのある国内の事業者等との連携を強化する。						
業績指標④	項目	基準					実績	
サイバーテロ(注2)の発生件数		22年度	23年度	24年度	25年度	26年度	22~26年度(平均)	27年度
	発生件数(件)	0	0	0	0	0	0	0
(28年4月警備企画課作成)								
注2: 重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いもの								
達成状況:○	達成目標	サイバーテロの発生及び被害の拡大を防止する。						

参考指標・参考事例	参考指標①	項目	22年	23年	24年	25年	26年	22~26年(平均)	27年
	サイバー犯罪等に関する相談受理件数	合計(件)	75,810	80,273	77,815	84,863	118,100	87,372	128,097
		詐欺・悪質商法	31,333	32,892	29,113	36,237	58,340	37,583	67,026
		迷惑メール	9,836	11,667	12,946	10,682	14,185	11,863	16,634
		名誉毀損・誹謗中傷	10,212	10,549	10,807	9,425	9,757	10,150	10,398
		不正アクセス・ウイルス	3,668	4,619	4,803	6,220	9,550	5,772	7,089
		インターネット・オークション	6,905	5,905	4,848	5,950	6,545	6,031	6,274
		違法情報・有害情報	3,847	3,382	3,199	3,132	5,080	3,728	4,854
		その他	10,009	11,259	12,099	13,217	14,643	12,245	15,822
	(28年4月情報技術犯罪対策課作成)								
参考指標②	項目	22年	23年	24年	25年	26年	22~26年(平均)	27年	
インターネット・ホットラインセンターが受理した違法情報及び有害情報件数	違法情報(件)	35,016	36,573	38,933	30,371	35,013	35,181	72,073	
	有害情報(件)	9,667	4,827	12,003	3,428	3,874	6,760	5,333	
(28年4月情報技術犯罪対策課作成)									

参考指標③	項目	22年	23年	24年	25年	26年	22～26年 (平均)	27年
出会い系サイト及びコミュニティサイトの利用に起因する犯罪に遭った児童の数	出会い系サイトの利用に起因する犯罪被害に遭った児童数(人)	254	282	218	159	152	213	93
	コミュニティサイトの利用に起因する犯罪被害に遭った児童数(人)	1,239	1,085	1,076	1,293	1,421	1,223	1,652
(28年4月情報技術犯罪対策課作成)								
参考指標④	項目	22年	23年	24年	25年	26年	22～26年 (平均)	27年
標的型メール攻撃の把握件数(注3)	標的型メール攻撃の把握件数(件)			1,009	492	1,723	1,075	3,828
	(28年4月警備企画課作成)							
注3: 警察と情報窃取の標的となるおそれのある事業者等との間でサイバー攻撃に関する情報共有を行う枠組みである「サイバーインテリジェンス情報共有ネットワーク」の連携事業者等(平成28年1月現在、7,333の事業者等)から報告を受けた件数								

業績目標達成のために
行った施策

<p>○ 「警察におけるサイバーセキュリティ戦略」の制定 社会情勢等の変化に的確に対応しつつ、サイバー空間の脅威に先制的かつ能動的に対処するため、警察庁において、27年9月、「警察におけるサイバーセキュリティ戦略」を制定・公表した。</p>
<p>○ 「サイバー空間の脅威への対処に係る人材育成方針」の策定 サイバー空間の脅威への対処に係る人的基盤を強化するため、警察庁において、27年12月、「サイバー空間の脅威への対処に係る人材育成方針」を策定・公表した。</p>
<p>○ 全国協働捜査方式の推進、捜査官の育成、各種資機材の整備等によるサイバー犯罪対策の体制の強化【行政事業レビュー対象事業:60 不正アクセス取締関係資機材の整備、61 サイバー犯罪取締りの推進】 IT社会における国民の安全・安心を確保するため、違法・有害情報の効率的な捜査活動を推進するための全国協働捜査方式(注4)を活用した取締りを推進した。また、サイバー犯罪対策に従事する警察職員に対し、サイバー犯罪対策に関する専門知識を習得させるための研修等を実施した。さらに、サイバー犯罪捜査や解析のために必要な資機材を整備するとともに、ファイル共有ソフトによるファイルの流通状況等の実態を把握するためのP2P観測システムを運用し、ファイル情報の分析・検索を行った。このほか、高度情報技術解析センターを中心に不正プログラムの効率的な解析を推進した。</p> <p>注4: インターネット・ホットラインセンターから警察庁に対して通報された違法・有害情報の発信元を割り出すための初期捜査を警視庁に設置された情報追跡班が一元的に行い、捜査すべき都道府県警察を警察庁が調整する捜査方式</p>
<p>○ 警察職員の研修等による警察のサイバー攻撃対策のための体制の強化【行政事業レビュー対象事業:64 サイバー攻撃対策の推進】 サイバー攻撃対策に従事する警察職員に対し、情報通信技術及びサイバー攻撃手法に関する民間委託研修等を実施したほか、新たな資機材を整備するなどし、サイバー攻撃の防御対策及び被害の拡大防止のための体制強化に努めた。</p>
<p>○ 予防・捜査等の推進に必要なインターネット観測の推進【行政事業レビュー対象事業:63 予防・捜査等の推進に必要なインターネット観測技術に関する調査研究】 リアルタイム検知ネットワークシステムを運用してサイバー攻撃の予兆及び実態の把握に努めるとともに、同システムの高度化に資するインターネット観測技術に関する調査研究を実施した。また、DoS攻撃等に係る観測機能強化を見据えた検討、開発及び試験運用を実施した。</p>
<p>○ 情勢に対応した訓練環境の充実【行政事業レビュー対象事業:62 情勢に対応した訓練環境の充実】 各種サイバー攻撃事案やサイバー犯罪事案を疑似的に体験できる訓練環境を用い、全国警察のサイバー攻撃対策やサイバー犯罪対策を担当する職員等に対して実践的な訓練を実施するとともに、新たな訓練シナリオを追加し、訓練環境を強化した。</p>
<p>○ 各種講演やセミナーによる研修及びホームページ等を活用した情報発信を通じた情報セキュリティ対策に関する広報啓発【行政事業レビュー対象事業:59 アクセス制御機能に関する技術の研究開発の状況等に関する調査及び広報啓発等】 警察やプロバイダ連絡協議会等が主催する研修会、学校等における講演会、情報通信技術関連イベント等における情報セキュリティ・アドバイザーによる講演やセミナーを実施したほか、警察庁ウェブサイトのサイバー犯罪対策のサイトや警察庁セキュリティポータルサイト(@police)、情報セキュリティ対策DVD、広報啓発用リーフレット等を通じて、情報セキュリティに関する広報啓発を行った。</p>
<p>○ サイバーテロ対策協議会、共同対処訓練等の実施による重要インフラ事業者等との連携強化 都道府県警察のサイバー攻撃対策プロジェクトにおいて、重要インフラ事業者等への個別訪問を行い、捜査に対する協力等の要請を行うとともに、サイバーテロ対策協議会、サイバー攻撃対策セミナー等を開催し、情報セキュリティに関する情報提供や意見交換等を行ったほか、重要インフラ事業者等と事案発生を想定した共同対処訓練を実施し、緊急対処能力の向上を図るなど、官民連携の強化に努めた。</p>

<p>○ 情報窃取の標的となるおそれのある事業者等との連携強化【行政事業レビュー対象事業:64 サイバー攻撃対策の推進】 情報窃取の標的となるおそれのある事業者等との「サイバーインテリジェンス情報共有ネットワーク」及びウイルス対策ソフト提供事業者等との「不正プログラム対策協議会」の枠組みを活用してサイバー攻撃に係る情報共有を行い、また、セキュリティ関連事業者と「サイバーインテリジェンス対策のための不正通信防止協議会」の枠組みを活用して官民の連携強化を推進した。</p>
<p>○ 国際捜査協力及び情報セキュリティに関する情報共有等によるサイバー犯罪取締り等のための国際連携の強化 G7ハイテク犯罪サブグループ会合やサイバー犯罪に係る二国間協議等への出席、アジア大洋州地域サイバー犯罪捜査技術会議の開催、国際刑事警察機構(ICPO)等を通じたサイバー犯罪・サイバー攻撃事案に係る国際捜査共助の実施等により、犯罪取締り等のための諸外国との国際連携を強化した。</p>
<p>○ 先進的なサイバー犯罪に対応するための効果的な抑止・捜査手法の活用 インターネットバンキングに係る不正送金事犯について徹底的な取締りを推進したほか、中継サーバー事業者等による不正アクセス禁止法違反事件等について効果的な取締りを実施した。また、サイバー犯罪の捜査情報を共有するシステムを運用し、各都道府県警察において個別に把握したサイバー犯罪に関する捜査情報等の共有を図り、合同・共同捜査を推進した。</p>
<p>○ 情報技術解析に係る関係機関との連携強化 デジタルフォレンジック連絡会を開催し、情報技術解析に係る関係機関との情報共有を図った。また、関係機関に対し、デジタルフォレンジックに関する講義を行うなどの取組を通じて連携強化を図った。さらに、インターネット上の脅威に係る技術情報の収集範囲の拡大を図るため、民間事業者等との協力関係構築に取り組んだ。</p>
<p>○ 総合セキュリティ対策会議の開催等による産業界等との連携強化【行政事業レビュー対象事業:59 アクセス制御機能に関する技術の研究開発の状況等に関する調査及び広報啓発等】 総合セキュリティ対策会議においては、「サイバー犯罪捜査及び被害防止対策における官民連携の更なる推進」について議論を行い、報告書等を取りまとめた。また、産学官連携によるサイバー空間の脅威への対処を目的とする一般財団法人日本サイバー犯罪対策センターの活動に参画した。さらに、不正アクセス防止対策に関する官民意見集約委員会(官民ボード)やプロバイダ連絡協議会等においてサイバー犯罪情勢や対策の在り方等について情報交換を行うとともに、インターネットに係る最新の技術に関する情報及び電子機器等の解析に必要な技術情報を得るため、民間企業との技術協力を推進した。</p>
<p>○ ホットライン業務の効果的な運用【行政事業レビュー対象事業:57 インターネット・ホットライン業務】 一般のインターネット利用者等から違法・有害情報に関する通報を受理し、警察への通報やサイト管理者等への削除依頼を行うため、警察庁が業務委託をしているインターネット・ホットラインセンターにおいて、通報を受けたインターネット上の違法・有害情報に関し、サイト管理者等に対して、27年中は違法情報32,534件、有害情報1,719件の削除依頼を行い、このうち違法情報30,359件(93.3%)、有害情報1,384件(80.5%)が削除された。</p>
<p>○ 外部委託したサイバーパトロール業務の効果的運用【行政事業レビュー対象事業:57 インターネット・ホットライン業務、58サイバーパトロール業務】 一般のインターネット利用者からの通報が期待できない出会い系サイトや児童ポルノ等が掲載された登録制サイト等をパトロールし、発見した違法・有害情報をインターネット・ホットラインセンターに通報するため、警察庁が業務委託しているサイバーパトロールにおいては、27年中に10,294件の通報を実施した。</p>
<p>○ インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律の効果的な運用 インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律に基づき、第6条の禁止誘引行為違反について、27年中は235件を検挙した。</p>
<p>○ サイバー防犯ボランティアの育成・支援【行政事業レビュー対象事業:57 インターネット・ホットライン業務】 サイバー空間におけるボランティア活動の促進を図るために作成した「サイバー防犯ボランティア活動のためのマニュアル(モデル)」、「サイバー防犯ボランティア育成のための研修カリキュラム(モデル)」を活用し、新たなサイバー防犯ボランティアの結成を促進するとともに、既存の防犯ボランティア団体の活動支援を推進した。</p>

評価の結果	各行政機関 共通区分	○:相当程度進展あり	
	目標の達成状況	<p>業績指標①については、27年中のサイバー犯罪の検挙件数(8,096件)が過去3年間の平均値(7,784件)と比較して増加し、目標を達成したが、サイバー犯罪等に関する相談受理件数(参考指標①)が増加していることに鑑み、おおむね目標を達成したものと評価する。</p> <p>業績指標②については、「実績」欄に掲げた事例を始めとする取組を推進し、情報セキュリティ事業者等との連携を強化したことから、目標を達成した。</p> <p>業績指標③については、27年度中、国内の事業者との連携を強化したことから、目標を達成した。</p> <p>業績指標④については、サイバー攻撃による脅威は依然として深刻であるものの、27年度中のサイバーテロの発生件数は0であったことから、おおむね目標を達成したと考えられる。</p> <p>各業績指標についてはおおむね目標を達成したものの、27年中は標的型メール攻撃の把握件数(参考指標④)が過去最多となり、日本年金機構を始めとする我が国の多数の機関、事業者等でサイバー攻撃による情報窃取等の被害が発生したほか、サイバー犯罪等に関する相談受理件数(参考指標①)が増加するとともに、インターネットバンキングに係る不正送金事犯による被害が過去最高となるなど、サイバー空間の脅威は依然として深刻であることから、基本目標である「安心できるIT社会の実現」の達成は道半ばであると考えられる。</p>	
	判断根拠		
達成状況の分析	<p>業績指標①については、上記の「業績目標達成のために行った施策」のうち、各種資機材がサイバー犯罪捜査において不可欠な資機材として活用されたことに加え、全国協働捜査方式の活用、ファイル共有ソフトを悪用した著作権侵害事犯の全国一斉取締り、捜査情報の共有、P2P観測システムの運用等の取組により、効果的かつ効率的な取締りが可能となったことから、当該取組が目標の達成に有効に寄与したと考えられる。</p> <p>また、インターネット・ホットラインセンターが受理した違法情報及び有害情報件数(参考指標②)は共に増加しており、インターネット・ホットラインセンターから警察庁への通報に基づく検挙も行われたことから、こうした外部委託業務も目標の達成に有効に寄与したと考えられる。</p> <p>業績指標②については、不正プログラムに感染している端末を把握した際に、国内の感染端末に係る情報をプロバイダに提供し、当該端末の利用者に対する注意喚起を官民連携して行ったことから、当該取組が目標の達成に有効に寄与したと考えられる。</p> <p>また、海外サーバ利用の違法アダルトアフィリエイトサイト(宣伝広告)に対する一斉集中取締りにおいては、一般財団法人日本サイバー犯罪対策センターから、違法サイトの絞込機能の高度化やウイルスの解析情報等に関する助言を得て捜査を進めたことから、当該取組も目標の達成に有効に寄与したと考えられる。</p> <p>業績指標③については、重要インフラ事業者等との共同対処訓練の実施や情報窃取の標的となるおそれのある事業者等との情報共有等の取組が、目標達成に寄与したと考えられる。</p> <p>業績指標④については、資機材の整備等により、サイバー攻撃対策の推進体制を強化したことや、共同対処訓練等により、重要インフラ事業者等や情報窃取の標的となるおそれのある事業者等との連携を強化したことのほか、リアルタイム検知ネットワークシステムを運用しサイバー攻撃の予兆及び実態の把握に努めたことが、目標の達成におおむね有効に寄与したと考えられる。</p>		
目標の達成状況及びその分析を踏まえた総括	<p>【業績目標】 今後も、安心できるIT社会の実現を目指すに当たり、サイバーセキュリティ基本法の施行等を踏まえる必要があることから、28年度の業績目標の表現を変更する。</p> <p>【業績指標及び達成目標】 業績目標の実現状況を評価するに当たり、サイバー犯罪の検挙件数等は業績指標として必ずしも適切でないところ、取組をより総合的に評価するため、業績指標を変更する。</p>	<p>【引き続き推進】 サイバー空間の脅威は依然として深刻であることから、引き続き、人的基盤の強化、各種資機材の整備等による捜査力及び解析力の強化、民間事業者、学識経験者、諸外国等との連携の強化、被害防止のための広報啓発の推進等に取り組む。</p>	
学識経験を有する者の知見の活用	28年6月17日に開催した第32回警察庁政策評価研究会において有識者の意見を聴取した上で作成した。		
政策評価を行う過程において使用した資料その他の情報	<ul style="list-style-type: none"> ○ 「平成27年におけるサイバー空間をめぐる脅威の情勢について」(28年3月警察庁) ○ 「インターネット・ホットラインセンターの運用変更について」(28年4月警察庁) ○ 「平成27年における出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について」(28年4月警察庁) 		
政策所管課	総務課、情報技術犯罪対策課、警備企画課、情報技術解析課	政策評価実施時期	27年4月から28年3月までの間