平成１５年

実績評価書

基本目標８　情報セキュリティを確保する
業績目標　ハイテク犯罪、サイバーテロ対策の推進

平　成　１　６　年　８　月
国家公安委員会・警察庁

はじめに

国家公安委員会及び警察庁における政策評価に関する基本計画においては、実績評価を実施する場合は、警察行政における主要な目標（基本目標）を設定し、当該基本目標を実現するための個別の政策が目指す具体的目標（業績目標）を選択し、業績目標ごとに設定した業績指標を１年以上の一定期間測定することにより、業績目標の実現状況を評価することとされている。

平成15年実績評価書においては、「基本目標８　情報セキュリティを確保する　業績目標　ハイテク犯罪、サイバーテロ対策の推進」について、平成13年から15年までの３年間を評価期間として業績指標を測定し、業績目標の実現状況を評価した。

基本目標８　情報セキュリティを確保する
業績目標　ハイテク犯罪、サイバーテロ対策の推進

(説明)
　捜査体制・技術支援体制の整備、諸外国・産業界との連携強化等を推進することにより、コンピュータ・ネットワーク上の治安維持を図り、国民が高度情報通信ネットワークを安心して利用することができるようにする。

評価期間　３年間(平成13年から15年まで)

業績指標
１　捜査体制・技術支援体制の整備状況を把握する。
　【施策】
(1)　ハイテク犯罪対策に係る体制整備
・　高度情報通信ネットワークの安全性確保のため、都道府県警察に対し、「平成14年生活安全警察(ハイテク犯罪対策関係)運営重点の実施細目について」(平成13年11月27日付け警察庁丁生企発第145号ほか)等により、ハイテク犯罪捜査官の採用、サイバーパトロール・モニターの委嘱等の推進を指示した。
・　サイバーパトロール(*1)を推進するため、平成15年、サイバーパトロールを行う都道府県警察職員及びサイバーパトロール・モニターに配布するためのマニュアルを作成した。
・　児童ポルノ事犯の取締りを推進するため、平成14年、児童ポルノ画像自動検索システム(*2)の運用を開始した。
(2)　サイバーテロ対策に係る体制整備
・　サイバーテロに的確に対応するため、平成13年、警察庁及び各管区警察局所属の高度な技術を有する者で構成した機動的技術部隊(サイバーフォース)を創設した。
・　サイバーテロ事案の未然防止及び拡大防止、迅速な事件検挙等を目的として、平成14年、警察庁にサイバーテロ対策推進室(*3)を設置するとともに、各都道府県警察にサイバーテロ対策プロジェクト(*4)を設置するよう指示した。

　【施策の効果】
(1)　ハイテク犯罪対策に係る体制整備
・　21都道府県警察において専門知識・技術を有する者21名がハイテク犯罪捜査官として中途採用された。これにより、高度な技術を利用した犯罪等に対し、より的確に対応することが可能となり、「不正アクセス行為の禁止等に関する法律」(平成11年法律第128号。以下「不正アクセス禁止法」という。)違反等

の事件が多数検挙された。

＜事例１＞　平成15年、インターネット・バンキングの口座開設者のＩＤとパスワードを収集し、架空名義で開設した自己の口座に送金操作を行った被疑者を不正アクセス禁止法違反、電子計算機使用詐欺等で検挙した。(警視庁)

＜事例２＞　平成15年、私立高校、コンピュータサービス会社及び病院が管理するウェブサーバに不正にアクセスし、ホームページ（ウェブサイトをいう。以下同じ。）を改ざんした被疑者を不正アクセス禁止法違反及び電子計算機損壊等業務妨害で検挙した。(警視庁)

・　15県警察においてサイバーパトロール・モニターの民間委嘱が実施された。また、警察庁作成のマニュアルを全国に配布した。これにより、インターネット上の違法・有害情報の収集が進み、ウェブ・サーバ管理者等への指導・要請が行われたほか、わいせつ物頒布等に係る事件が検挙された。

その一方、サイバーパトロール・モニターの民間への委嘱が進んでいない都道府県警察が多数あるほか、学識経験を有する者から、インターネット上にはまだ多くの違法・有害情報がはん濫していることから、サイバーパトロール活動が十分とは言えないとの指摘があった。

＜事例３＞　平成14年、「殺人依頼」と題するインターネット上の掲示板に殺害対象として個人の住所、氏名が書き込まれているのを発見したとのサイバーパトロール・モニターの報告を受け、掲示板管理者に書き込みを削除するよう要請した。(長野)

＜事例４＞　平成14年、インターネットオークションでわいせつＣＤ－Ｒが販売されているのをサイバーパトロール・モニターが発見し、これを端緒として、わいせつ物頒布等で被疑者を検挙した。(熊本)

・　児童ポルノ画像自動検索システムの運用により、事件を検挙したほか、海外のサーバにある児童ポルノ画像を平成14年には21件、平成15年には23件発見し、ＩＣＰＯを通じて関連する国々に情報提供した。

児童ポルノ画像自動検索システムによる発見を端緒とした事件検挙は少ないが、その理由として、運用開始後間もないために、未だ十分な数の児童ポルノ画像が登録されていないことが挙げられる。

＜事例５＞　平成14年、児童ポルノ画像自動検索システムによりホームページ上の児童ポルノ画像を発見し、これを掲示していた被疑者を児童ポルノ公然陳列等で検挙した。(山形)

(2)　サイバーテロ対策に係る体制整備

・　サイバーフォースの設置により、重要インフラ事業者等の責任者が講ずべき対策に関する指導・助言のほか、技術情報の提供、ペネトレーションテスト(*5)の実施が可能となった。

　平成14年に比べ、平成15年は重要インフラ事業者等からのペネトレーションテストの要請が減少しているが、警察庁では、重要インフラ事業者等に対し、自主的なペネトレーションテストの実施を勧めているところである。

　今後も、自主的なペネトレーションテストを実施していない重要インフラ事業者等を中心に、その意義等を教示する目的でペネトレーションテストを行っていく予定である。

＜サイバーフォースの活動件数＞

	平成14年	平成15年
指導・助言	967件	1,267件
技術情報の提供	402件	244件
ペネトレーションテスト	103件	21件
活動件数(合計)	1,472件	1,532件

・　すべての都道府県警察にサイバーテロ対策プロジェクトが設置された。これにより、平素から緊急対処(*6)に必要な各種情報技術を共有し、緊急対処時には素早い連絡を可能にする連絡窓口457拠点が全国の重要インフラ事業者等に設置された。

2　ハイテク犯罪について、その検挙件数を継続的に測定するなどにより、検挙状況を把握する。

【施策】

・　捜査体制・技術支援体制の強化(業績指標１参照)
・　情報セキュリティ水準の向上(業績指標３参照)
・　警察職員に対する研修の実施(業績指標５参照)
・　近年のハイテク犯罪の発生状況等を踏まえ、都道府県警察に対し、「平成14年生活安全警察(ハイテク犯罪対策関係)運営重点の実施細目について」(平成13年11月27日付け警察庁丁生企発第145号ほか)等により、ハイテク犯罪捜査の推進を指示した。

【施策の効果】

・　評価期間を通じてハイテク犯罪の検挙件数は一貫して増加していることから、捜査体制・技術支援体制の強化、警察職員に対する研修の実施、通達によるハイテク犯罪捜査の推進の指示は、効果を上げていると認められる。

＜ハイテク犯罪の検挙件数＞

	12年	13年	14年	15年
不正アクセス禁止法違反	67	67	105	145
コンピュータ・電磁的記録対象犯罪	44	63	30	55
電子計算機使用詐欺	33	48	18	34
電磁的記録不正作出・毀棄	9	11	8	12
電子計算機損壊等業務妨害	2	4	4	9
ネットワーク利用犯罪	802	1,209	1,471	1,649
児童買春	8	117	268	269
児童ポルノ	113	128	140	102
青少年保護育成条例違反	2	10	70	120
わいせつ物頒布等	154	103	109	113
詐欺	306	485	514	521
名誉毀損	30	42	27	46
著作権法違反	80	86	66	87
脅迫	17	40	33	38
その他	92	198	244	353
合計	913	1,339	1,606	1,849

3　情報セキュリティ水準を向上させるための活動状況を把握する。

【施策】

(1)　広報啓発活動の推進

・　国民の情報セキュリティ意識の向上を図るため、平成15年、警察庁セキュリティポータルサイト(@police)(*7)を開設し、情報セキュリティに係る注意喚起や情報提供を実施している。

　また、インターネット定点観測(*8)の情報提供を開始し、インターネットの情勢をリアルタイムに広報している。

・　国民の情報セキュリティ意識の向上を図るため、「我が国におけるインターネット治安情勢の分析について」を平成14年から年報等で公表している。

・　国民の情報セキュリティ意識の向上を図るため、広報啓発ビデオ「虚構からの誘惑」等を監修・製作した。

・　国民の情報セキュリティ意識の向上を図るため、全国警察を挙げて「ハイテク犯罪防止のための情報セキュリティ対策」の広報啓発を重点的に実施した。

・　アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、国家公安委員会、総務大臣及び経済産業大臣は、不正アクセス禁止法第７条に基づき、「不正アクセス行為の発生状況及びアクセス制御機能の技術の研究開発の状況」を公表した。

・　不正アクセス禁止法第６条の援助規定に基づくアクセス管理者に対する助言・

指導を適正に実施するため、都道府県警察に対し、「不正アクセス禁止法第６条の援助に関する留意事項について(改正)」(平成13年４月１日付け警察庁丁生企発第38号ほか)により、その実施に当たっての留意事項を通達した。

(2)　広報啓発活動のための体制整備等

・　国民がハイテク犯罪の被害に遭わないための広報啓発活動を推進するため、都道府県警察に対し、「情報セキュリティアドバイザーの活動指針等について」(平成13年３月27日付け警察庁丁生企発第32号)等により、情報セキュリティアドバイザー(*9)の配置の推進を指示するとともに、平成13年度地方財政計画において、配置に係る経費を措置した。

・　ハイテク犯罪の被害相談等に適切に対応するため、都道府県警察のハイテク犯罪相談窓口の存在を警察庁ホームページ等で広報しているほか、都道府県警察に対し、「情報セキュリティアドバイザーの活動指針等について」等により、相談業務を積極的に広報して相談窓口の利用を促進するよう指示した。

・　ハイテク犯罪の最新の手口を踏まえた情報提供等を推進するため、各都道府県警察に対し、「情報セキュリティアドバイザーの活動指針等について」等により、情報セキュリティコミュニティセンター(*10)の設置・活用を指示した。

【施策の効果】

(1)　広報啓発活動の推進

・　警察庁セキュリティポータルサイト(@police)においてセキュリティインシデント(*11)の解析結果78件を広報したほか、広報啓発ビデオ等を作成した。@policeやこれら広報啓発ビデオ等は、各種メディアでも取り上げられている。

・　不正アクセス禁止法第６条の援助規定については、警察庁が示した留意事項に基づき、次のとおり実施されている。

＜都道府県公安委員会による援助措置件数＞

都道府県公安委員会による援助措置件数	12年	13年	14年	15年
	6	21	5	5

＜事例６＞　平成15年、ホームページに不正な書き込みを受けた大学から援助の申出を受けたことから、公安委員会が不正アクセス禁止法に基づく援助として、不正アクセスの手口等の分析、再発防止対策等の指導を行った。

(2)　広報啓発活動のための体制整備等

・　24都道府県警察に情報セキュリティアドバイザー29名が配置され、国民から

のハイテク犯罪等に関する相談に対応しているほか、情報セキュリティに関する広報啓発等が推進されている。

＜事例７＞　平成14年、県内の自治体、企業、大学等に働きかけ、全県的なネットワーク網を構築し、情報セキュリティアドバイザーが開発した「ホームページ改ざん情報自動通報ツール」により不正アクセス被害に係る通報を同ネットワーク上で開始した。これにより、各種情報セキュリティに関する情報が共有できるようになった。(茨城)

＜事例８＞　平成14年、３か月にわたり毎週日曜日に地方紙に「最新とくしまＩＴ事情・犯罪編」を連載し、インターネットオークション利用時の注意点、不正アクセス対策等を県民に分かりやすく紹介した。(徳島)

・　ハイテク犯罪等に関する相談受理件数は、インターネット利用人口の増加等の影響を受け、次のとおり増加しており、ハイテク犯罪相談窓口の存在について周知が進んでいると認められる。

その一方で、学識経験を有する者から、警察署等におけるハイテク犯罪に関する相談対応について、窓口ごとにばらつきがあることから、警察内部で更に連携等を図る必要があるとの指摘もなされている。

＜ハイテク犯罪等に関する相談受理件数＞

	12年	13年	14年	15年
詐欺・悪質商法に関する相談	1,396	1,963	3,193	20,738
うち架空請求メールに関する相談	-	-	-	17,838
インターネット・オークションに関する相談	1,301	2,099	3,978	5,999
違法・有害情報に関する相談	2,896	3,282	2,261	4,225
名誉毀損、ひぼう中傷等に関する相談	1,884	2,267	2,566	2,619
迷惑メールに関する相談	1,352	2,647	2,130	2,329
不正アクセス、コンピュータ・ウイルスに関する相談	505	1,335	1,246	1,147
その他	1,801	3,684	3,955	4,697
相談受理件数（合計）	11,135	17,277	19,329	41,754

（注）　架空請求メールに関する相談は、詐欺・悪質商法に関する相談として扱われている。平成15年に同相談が急増したことから、内数として集計を開始したもの。

・　警視庁のほか、６県警察で情報セキュリティコミュニティセンターを活用した広報啓発活動が実施されている。

他方、学識経験を有する者から、子ども向けの広報啓発活動等、国民の幅広い要望に応えられる広報啓発活動を更に推進するべきであるとの指摘もなされ

ている。

＜事例９＞　平成15年、学校関係者、自治体、民間企業等66団体90名を対象としたセミナーを開催し、情報セキュリティに関する情報提供を行った。同セミナーについては、新聞で広報されたほか、アンケート結果も良好であった。(注)(青森)

(注)　アンケート結果は、「非常に良い」「良い」を合わせて77.7%(講演)、85.9%(実演)であった。

＜事例10＞　平成15年、情報セキュリティアドバイザーが中心となり、地方公共団体、企業のネットワーク管理者等延べ112名を対象としたセミナーを開催し、情報セキュリティに関する情報提供を行った。同セミナーについては、地元のテレビで広報されたほか、アンケート結果も良好であった。(注)(沖縄)

(注)　アンケート結果は、「非常に良い」「良い」を合わせて68.6%(講演)、89.7%(Windows実習)、82.7%(Linux実習)であった。

・　情報セキュリティ水準の向上に係るこれらの施策が、どの程度、国民の情報セキュリティ意識の向上につながっているかを計測することは困難である。しかし、国家公安委員会・総務省・経済産業省が発表している不正行為アクセスの認知件数は、平成13年の1,253件から平成14年には329件、平成15年には212件と年々減少しており、これは、当庁を含め、官民を挙げて広報啓発活動を実施したことによる効果がその要因の一つであると考えられる。同様の見解は、「平成15年情報通信に関する現状報告」(総務省)においても示されているところである。

この一方で、コンピュータ・ウイルス対策等の情報セキュリティ対策をインターネット利用者の３分の１が実施していないとの報告(注)もあることから、引き続き、情報セキュリティ水準の向上を図っていく必要がある。

(注)　インターネット利用者の33.6%が情報セキュリティ対策を何も実施していない。(総務省「平成15年情報通信に関する現状報告」)

４　不正アクセスに対する監視・緊急対処体制の整備状況を把握する。

【施策】

・　サイバーテロの予兆を早期に発見するため、平成13年、攻撃の兆候をリアルタイムに検知・通報するネットワークシステムを整備した。
・　不正アクセスの痕跡から攻撃手法を特定して迅速・的確に防御策を講ずるため、不正アクセス手法等の検証作業を実施した。
・　コンピュータ・ウイルス等に対する防御策を講ずるため、その機能と対策を検証するための資機材等を整備した。
・　警察職員に対する研修を実施した。(業績指標５参照)

【施策の効果】

・　インターネットの情勢をリアルタイムに把握できる環境の整備に加え、独自にコンピュータ・ウイルス等を解析・検証できる能力を備えたことにより、高度かつ複雑な機能を有するコンピュータ・ウイルスや海外を経由して時間的制約なしに発生する不正アクセス等に対し、適切に防御策を講ずることが可能となった。

＜事例11＞　平成15年、特定のサーバに対してサイバー攻撃を行うようプログラムされていたブラスターワーム(*12)が世界規模でまん延した事案に対して、警察庁は、当該コンピュータ・ワームが悪用するＯＳのぜい弱性に関する情報をまん延以前の段階で迅速に収集したことにより、まん延初期段階で独自の解析により得られた当該コンピュータ・ワームの動作・感染能力及び対策に係る情報を国民に提供することができた。

5　警察職員に対する研修状況を把握する。

【施策】

(1) ハイテク犯罪対策に係る研修状況

・　警察庁、管区警察局及び都道府県警察において、ハイテク犯罪対策に従事する警察官及び技術職員を対象として、ハイテク犯罪の防止及び捜査を行うために必要となる手続や技術的知識を習得させるための研修を124回(警察庁23回、その他101回)実施した。

(2) サイバーテロ対策に係る研修状況

・　警察庁において、サイバーテロ対策に従事し、又は従事する予定のある警察官及び技術職員を対象として、サイバーテロの未然防止策及び関連事案の捜査に関する基礎知識・技能を習得させるための研修を３回実施した。

※　参加人数：警察庁38名、その他25名

・　警察庁において、全国の都道府県警察のサイバーテロ対策要員(警察官)を対象に、サイバー攻撃の防御、サイバー攻撃の有無の確認等に関する知識・技能を習得するための民間委託研修を含む研修を実施した。

※　研修期間：平15.11月～12月の７週間　参加人数：45名　計92名

平14.２月～３月の６週間　参加人数：47名

・　警察庁において、民間委託研修を修了したサイバーテロ対策要員(警察官)を対象に、サイバー攻撃及びその防御等に係るサイバーテロ対策訓練を実施した。

※　訓練期間：平成14年11月の２週間　参加人数：44名

・　警察庁及び管区警察局のサイバーフォース要員に対して、情報通信システムを構成するハードウェア、ＯＳ、各種アプリケーションに係る詳細な知識等民

間の最先端技術を習得させるための研修・訓練を実施した。

※　参加人数：サイバーフォース要員　延べ202名

研修期間：H15.9月～12月の11週間　参加人数：31名

H15.１月～３月の12週間　参加人数：36名

H14.11月～12月の４週間　参加人数：10名

H14.９月～11月の10週間　参加人数：14名

H14.１月～３月の10週間　参加人数：56名

H13.12月の２週間　参加人数：16名

H13.９月～11月の９週間　参加人数：39名

・　米国及び英国の捜査機関等に、延べ42名のサイバーフォース要員を派遣し、ハイテク犯罪への技術的対応に関する訓練を実施した。

【施策の効果】

・　研修を受けた職員が中心となって対応した結果、業績指標２のとおり、評価期間を通じてハイテク犯罪の検挙件数は増加していることから、ハイテク犯罪対策に係る研修は、効果を上げていると認められる。

・　研修を受けた職員が中心となって対応した結果、評価期間中に発生したワーム等を解析・検証し、国民への注意喚起を実施できたことから、サイバーテロ対策に係る研修は、効果を上げていると認められる。

＜事例12＞　平成14年２月～３月、全国の都道府県警察のサイバーテロ対策要員(警察官)47名を対象とした研修を実施したことにより、これら参加者のサイバー攻撃に対する防御等に関する知識・技能を高めることができた。(注)

（注）サイバー攻撃に対する防御等に関する知識・技能に関し、テストを３回実施したところ、研修前の事前テストでは参加者47名の平均正答率は約22%であったが、研修後の最終テストでは平均正答率が約92%となった。

＜事例13＞　平成15年、スラマーワーム(*13)により韓国のインターネットに大規模な障害が起きた事案に対し、各種研修を受けた、サイバーフォースやサイバーテロ対策プロジェクト要員を始めとするサイバーテロ対策に従事する全国の警察職員が、情報収集を迅速に進めるとともに、重要インフラ事業者等と緊密に連携を図り、我が国の被害を未然に防止すべく、これを解析・検証し、国民に注意喚起することができた。

6　諸外国の関係機関及び産業界との連携状況を把握する。

【施策】

(1) 諸外国の関係機関との連携

ア　ハイテク犯罪に係る国際会議

・　Ｇ８国際組織犯罪対策上級専門家会合(リヨン・グループ)ハイテク犯罪サブグループに参加している。平成15年における参加状況は次のとおり。

開催地：パリ(２月、４月、11月)

内　容：重要インフラ防護に関する原則の策定、国家間の緊急連絡網の実効性向上等

参加者：Ｇ８各国、ＥＵ等(警察庁からは生活安全企画課、技術対策課等の担当官が参加)

・　アジア地域サイバー犯罪捜査技術会議を開催した。(平成15年２月)

主　催：警察庁

開催地：東京

内　容：ハイテク犯罪に関する各国の情勢及び対策並びに効果的な技術等の情報交換

参加者：アジア９か国・１地域等

イ　24時間コンタクトポイントによる諸外国との連携

・　Ｇ８各国と連携し、国家間の緊急連絡網の実効性向上を目的とした24時間コンタクトポイントのテストに参加した。(平成15年)

・　警察庁が中心となってアジア諸国警察機関との連携を確保するため、平成13年、24時間連絡が取れる手段としてサイバー犯罪技術情報ネットワークシステム(CTINS(*14))を設置し、その運用を通じて、サイバー犯罪対策に係る技術情報の共有を行った。

※　参加国：９か国・１地域(日本を含む。)

ウ　諸外国の関係機関との連携

・　米国捜査機関からの研修生２名を受け入れ、ハイテク犯罪対策、サイバーテロ対策に関する訓練を実施した。

(2) 産業界等との連携

・　情報セキュリティの有識者らで構成される「総合セキュリティ対策会議」を開催した。

・　都道府県警察に対し、ハイテク犯罪情勢や犯罪実態に係る情報交換を行うため、プロバイダ等との連絡協議会を設置し、効果的な活動を図るよう指示した。

・　緊急対処に必要な各種情報技術の共有、緊急対処時の素早い連絡、情報セキュリティ対策の自主的な取組みの要請等、重要インフラ事業者等との連携を図るべく、都道府県警察のサイバーテロ対策プロジェクト等に、重要インフラ事業者等との連絡窓口を設置するよう指示した。(業績指標１参照)

・　都道府県警察に対し、民間企業、重要インフラ事業者等が参加するサイバーテロ対策協議会を設置するなど、効果的な活動を図るよう指示した。

・　サイバーフォース要員を大学の研究室に派遣してリアルタイム検知ネットワークに係る共同研究を実施するとともに、民間企業とコンピュータ防御技術・情報収集に関する共同研究を実施した。

【施策の効果】

(1) 諸外国の関係機関との連携

・　各種会議やCTINS等を通じ、諸外国の関係機関との連携が進んでいる。

＜事例14＞　平成15年、CTINSを活用して韓国の警察庁と情報交換を行い、京都市内の病院が管理するウェブサーバに不正にアクセスしてホームページを改ざんした被疑者を検挙した。(警視庁)

・　アジア地域サイバー犯罪捜査技術会議やCTINSの設置・運用を通じ、アジアを中心とした情報共有の枠組みの確立を進めてきた。

その結果、平成15年には英国が当該会議への参加を要請するなど、アジア以外の国からも関心を持たれており、当該枠組みが国際的に評価を受けつつあるものと考えられる。

(2) 産業界等との連携

・　総合セキュリティ会議において、警察と産業界等との連携の在り方について検討し、「情報セキュリティ対策における連携の推進について」(平成14年)及び「情報セキュリティに関する脅威の実態把握・分析について」(平成15年)を報告書としてまとめた。

・　多数の都道府県警察においてプロバイダ等連絡協議会が設置され、全国計58回開催され、情報交換等が行われている。

＜事例15＞　平成14年、福島県ネットワーク・セキュリティ連絡協議会総会が開催された。同総会では、平成13年度の活動報告が行われたほか、平成14年度活動計画として、社内のコンピュータ・ネットワークの総点検の実施、関係者のメーリングリストの構築等が承認された。同総会は、新聞でも報じられ、県民にも周知されている。（福島）

・　平素から緊急対処に必要な各種情報技術を共有し、緊急対処時には素早い連絡を可能にする連絡窓口457拠点が全国の重要インフラ事業者等に設置された。(業績指標１参照)

＜事例16＞　ワールドカップサッカー大会開催に当たり、サイバーテロの発生が懸念され、それに伴う情報通信網の機能不全が大会運営に重大な

支障を及ぼすおそれがあったことから、サイバーフォース及び都道府県警察の職員が大会関連施設及び重要インフラ事業者等を訪問し、サイバーテロ対策の指導・助言を行うとともに、FIFAワールドカップ日本組織委員会等の要請を受けてペネトレーションテストを実施するなど、事前対策に努めた。

また、開催期間中、警察庁では、サイバー攻撃に対する監視体制を強化するとともに、サイバーテロが発生したときに備え緊急対処体制を設置した。

・ 警視庁、大阪府警察、広島県警察及び香川県警察に、サイバーテロ対策協議会が設置され、警察のサイバーテロ対策の説明、サイバー攻撃事案の事例紹介(データ流出事案、不正アクセス事案等)等の情報交換が行われている。

また、協議会会員を参加者とするメーリングリストを構築したところ、平素から協議会会員同士で情報セキュリティに関する自主的な情報交換が行われており、警察及び協議会会員の連携は深まりつつあると考えられる。

なお、未だ多数の府県警察にサイバーテロ対策協議会が設置されていないが、府県によっては、重要インフラ事業者等の数が少ないため、そのような地域にあっては、連絡窓口を通じて連携を図っていくこととしている。

・ 共同研究により得られた成果を@policeにおいて広く公開したほか、自主的な情報セキュリティ対策に資するため、技術的なノウハウを重要インフラ事業者等に提供した。また、共同研究の成果を活用し、サイバーフォースにおける緊急対処活動の高度化を図っているところである。

参考指標

＜インターネット利用者数＞

	９年	10年	11年	12年	13年	14年	15年
利用者数(万人)	1,155	1,694	2,706	4,708	5,593	6,942	7,730

出典：総務省「平成15年通信利用動向調査」

学識経験を有する者の知見の活用に関する事項

この評価書は、有限責任中間法人JPCERTコーディネーションセンター代表理事歌代和正氏、特定非営利活動法人日本ガーディアン・エンジェルス理事長小田啓二氏、東京電機大学工学部教授佐々木良一氏らの意見を聴取するとともに、平成16年６月23日に開催した警察庁政策評価研究会において意見を聴取した上で作成した。

評価の結果

・ 高度情報通信ネットワーク社会に移行しつつある現在、増加基調にあるハイ

テク犯罪を抑止し、はん濫する違法・有害コンテンツによる害悪を抑制することは、国民がインターネットを安心して利用するために必要不可欠であるため、ハイテク犯罪対策を推進する必要性が認められるところである。

また、電力・ガス等の重要インフラ事業者等の基幹システムがサイバー攻撃を受けた場合、国民生活や社会経済活動に重大な支障を及ぼすことが懸念されることから、サイバーテロ対策を推進する必要性が認められるところである。

・ 学識経験を有する者から、サイバーパトロール活動が十分とは言えないとの指摘や、ハイテク犯罪相談について警察内部で更に連携等を図るべきとの指摘、情報セキュリティに関する広報啓発活動で子ども向けのものが少ないなどの指摘がなされている。これらの指摘はあるものの、前述の業績指標で示したとおり、捜査体制・技術支援体制の整備、警察職員の能力向上により、ハイテク犯罪の検挙件数は年々増加しているほか、不正アクセスへの監視・緊急対処体制の整備、諸外国・産業界との連携強化が一定の効果を現していることから、本政策はおおむね有効であったと評価し得る。

・ 他方、今後もインターネットの利用者の増加(注)に伴い、ハイテク犯罪も増加することが予想されることから、ハイテク犯罪対策の必要性はますます高まるといえる。

また、テロ情勢の緊迫化、高度情報通信ネットワーク社会の安全性・信頼性を脅かす事案の続発等、サイバーテロの脅威が現実のものとなりつつある中、サイバーテロ対策を更に強化していくことが求められている。

（注） 平成19年のインターネット利用者数は8,892万人に達すると予想されている。(総務省「平成15年情報通信に関する現状報告」)

・ よって、本政策は今後も継続して実施すべきである。

政策所管課：総務課

*1 サイバーパトロール：ネットワーク上を流通する違法・有害情報を把握し、違法・有害情報の流通による害悪の発生の防止を図る活動。

*2 児童ポルノ画像自動検索システム：インターネット上にある画像の中から、都道府県警察が登録した児童ポルノ画像と同一の画像を自動的に検索するシステム。

*3 サイバーテロ対策推進室：サイバーテロ対策を総合的に推進するため、警察庁に設置された体制。警察庁情報通信局情報通信企画課長を室長、同技術対策課長を副室長とし、警備局警備企画課等の要員で構成。重要インフラ事業者の基幹システムに対する電子的攻撃又は重大な障害で電子的攻撃による可能性が高いものに関して、平素から情報収集を推進し、サイバーフォース、サイバーテロ対策プロジェクトとの情報の共有を図る。また、事案が発生した場合に、緊急対処活動として、サイバーテロ対策プロジェクト及びサイバーフォースが重要インフラ事業者等に対し被害の拡大防止、被害復旧等のための指導・助言等を実施したときには、当該事案に関する情報を収集・分析し、関連するサイバーテロ対策プロジェクト等に対し必要な指導・調整を行うなどしてい

る。

*4　サイバーテロ対策プロジェクト：サイバーテロ対策の推進のため、都道府県警察において、当該都道府県警察職員と都道府県通信部職員が連携して確立する体制。サイバーテロ対策推進室、サイバーフォースと情報の共有を図りつつ、事案発生時の緊急対処活動等を実施する。

*5　ペネトレーションテスト：インターネット等外部に公開しているサーバコンピュータや社内ネットワークのコンピュータを不正侵入者から守るため、ネットワーク全体の安全性の検証を行うこと。

*6　緊急対処：サイバー攻撃のおそれが高い又は実際に被害が生じた場合に、速やかに現場臨場し、事案発生の未然防止、被害の拡大防止を図る活動。具体的には、攻撃を防御するための情報を提供し、攻撃対象となっているシステムの堅牢化を技術的に支援するとともに、被害が生じている場合には、その復旧支援に当たる。

*7　警察庁セキュリティポータルサイト(@police)：警察に集約された情報セキュリティに関する情報をいち早く提供し、インターネット利用者のセキュリティ意識の向上並びにサイバー犯罪及びサイバーテロの未然防止を図るために公開された警察庁ホームページ。

*8　インターネット定点観測：全国の警察施設に設置された不正侵入検知システム及びファイアウォールで検出したアクセスを警察庁において集計・統計処理を施し、グラフ化したもの。

*9　情報セキュリティアドバイザー：国民からのハイテク犯罪等に関する相談への対応、地方公共団体、学校、民間企業等に対する情報セキュリティに関する広報啓発及びハイテク犯罪対策に関する産業界との連携等ハイテク犯罪の予防に資する施策の推進に従事する者。

*10　情報セキュリティコミュニティセンター：学校教育関係者、地方公共団体職員、一般国民等に対し、警察がハイテク犯罪予防のための助言・指導を行い、自主的な情報セキュリティ対策を促すための情報提供の場。

*11　セキュリティインシデント：コンピュータ・ウイルス、コンピュータ・ワーム等、インターネットにおいて発生した情報セキュリティの脅威となる事案。

*12　ブラスターワーム：平成15年８月、世界的にまん延したコンピュータ・ワーム。特定のＯＳのぜい弱性を有するコンピュータに侵入し、更に同様のぜい弱性を有する他のコンピュータを探し、同様の感染活動を繰り返すことにより感染が拡大する。ネットワークに負荷をかけるとともに、特定のコンピュータに対してDoS攻撃を行うようプログラムされていた。

*13　スラマーワーム：平成15年１月、韓国において大規模なインターネット接続障害を発生させたコンピュータ・ワーム。特定のサーバソフトのぜい弱性を悪用してサーバに侵入し、さらに他のサーバへ同様の侵入を繰り返すことにより、トラフィックを増大させ、システムダウンを引き起こす。

*14　CTINS：ハイテク犯罪の技術的手口やデジタル証拠の解析手法のほか、警察庁においてモニターしているインターネット上の悪意ある活動（コンピュータ・ウイルスやコンピュータ・ワーム等）について情報共有を行うため、アジア諸国9か国・１地域（日本を含む。）の法執行機関を結んだネットワーク・システム。