政策の名称	サイバーテロ対策（サイバーテロ対策用資機材の整備、サイバーテロ対策要員の能力向上）
政策の内容・目的	サイバーテロの未然防止及び事案発生時の的確な対処のため、サイバーテロを敢行するおそれのあるテロ組織等に関する情報収集体制の強化及び重要インフラの管理者との連携強化を図る。 この目的のため、平成14年度において、次のような施策を講じる。 (1) サイバーテロ対策要員の育成 (2) 重要インフラとの連携強化等を行うための資機材の整備 (3) テロ組織等に関して収集した情報を分析するための情報分析システムの整備
必　要　性	情報通信技術の発展とこれに伴う高度情報通信ネットワーク社会の進展により、コンピュータ・ネットワークが行政、重要インフラ等の公共性の高い社会基盤に浸透している。こうした中で、平成12年１月には中央省庁ホームページ改ざん事件が発生し、また、同年２月にはオウム真理教関連のソフトウェア会社が官公庁や公益性の高い企業のシステム開発に携わっていたことが明らかになるなど、政府機関や重要インフラに対するサイバーテロの脅威が現実のものとなりつつある。 このような情勢下、平成12年12月には全省庁が参加する情報セキュリティ対策推進会議において「重要インフラのサイバーテロ対策に係る特別行動計画」が策定されるなど、サイバーテロ対策は政府の重要課題となっている。特に、平成13年３月に高度情報通信ネットワーク社会推進戦略本部が策定したe-Japan重点計画には、警察庁が実施しなければならない重要インフラのサイバーテロ対策の一つとして「テロ組織等に関する情報収集体制の整備、警察と重要インフラ管理者との連携強化、要員の技術の向上を図る」ことが盛り込まれている。
達成効果等	平成14年度予算により上記(1)～(3)の施策を講じることができれば、次のような効果が期待される。 (1) 各都道府県警察において、重要インフラの管理者に対し、情報セキュリティに関する基礎的な助言を行うとともに、サイバーテロが発生した際、第一次的な対処を行うことが可能な捜査員の育成が図れる。 (2) 平成11年度及び平成12年度に特に必要性の高い県警察にテロ組織に関する情報収集及び重要インフラとの連携強化を図るための資機材を整備しており、下記のとおり高い効果を示している。資機材既整備県以外の県で、重要インフラが多く所在している県にも既整備県に準ずる資機材を整備することにより、重要インフラの管理者との連携が一層強化されるとともに、インターネットを通じた情報収集体制が強化される。 【参考】（既整備資機材の設置効果） ● テロ組織に関する情報収集に関しては、平成12年２月にオウム真理教の関連ソフトウェア会社が官公庁や公益性の高い企業のシステム開発に携わっていたこと

	を解明するなどの成果を上げている。 ● 重要インフラとの連携強化についても、関連情報の提供や連絡体制の確立等の対策を着実に推進しており、平成12年７月の九州・沖縄サミットの開催に際しては、サイバーテロの未然防止及び発生時の的確な対処のため、警備諸対策の一環として、重要インフラ等との連携を図り、サイバーテロを完全に封圧した。 (3) テロ組織等について収集した膨大な情報を管理し、事件発生時において、類似性、容疑性を照合してわずかな端緒から的確に捜査資料を引き出したり、複数の捜査員によって同時並行的に押収した電磁的記録物の分析を行う環境が整い、より確実なサイバーテロの予兆の把握、対処が可能となる。
予　算　額	平成14年度要求・要望額　　132百万円
効　率　性	本施策は、費用対効果を配慮して、以下のとおり要求額を最低限必要とされる額に絞り込んでおり、非常に効率的である。 (1) 全国の県警察において早急なサイバーテロ対策要員の能力向上が必要とされているところ、各県警で対策の核となるべき要員のみを育成の対象とすることにより、必要最低限の人員に絞っている。 (2) 重要インフラとの連携強化に必要な資機材の整備対象県は、これまで資機材を整備していない県であって、かつ、重要インフラが多く所在する県を厳選している。 (3) 情報分析システムの整備対象県は、これまでに各県警察が収集したテロ組織に関する情報の質及び量を考慮し、効率的な情報の整理及び的確な分析のため、システムの整備が不可欠と認められる県を厳選している。
そ　の　他	

政策所管課	警備企画課	政策評価実施時期	平成13年８月

平成１３年８月

我が国における不正アクセス行為等の発生状況

１　警察の不正アクセス行為の認知状況

（平成１２年２月１３日～平成１２年１２月３１日　約１１ヶ月）

○　不正アクセス行為の認知件数　１０６件　（うち２５件は海外からと判明）

- ホームページの改ざん、消去を伴うもの　　３３件
- ＤＤｏＳ用攻撃ツールが仕掛けられていたもの　　２件

２　情報処理振興事業協会（ＩＰＡ）に届出のあったコンピュータ不正アクセスの状況

（平成１２年２月１３日～平成１２年１２月３１日　約１１ヶ月）

○　コンピュータ不正アクセス被害届出件数　１２８件

- 権限取得行為（侵入行為）　　３６件

３　コンピュータ緊急対応センター（JP-CERT/CC）に届出があった不正アクセス関連行為（平成１２年２月１３日～平成１２年１２月３１日　約１１ヶ月）

○　届出のあった不正アクセス関連行為　　２０８４件

- システムへの侵入　　１０６件
- サービス不能攻撃　　２９件

平成１３年８月

海外におけるサイバーテロ関連事案（サイバー攻撃事案）

発　生　年	概　　要
１９９０年４月 ～　１９９１年５月	オランダのハッカー数名が国防総省施設３４箇所のコンピュータシステムに侵入し、システムの改ざん等を行った。
１９９４年３月、４月	ニューヨーク州にある米空軍の研究施設であるローム研究所が、インターネットを通じて１５０回以上もの攻撃を受けた。
１９９４年６月	ロシア人グループがアメリカ所在のシティ・バンクに不正アクセスし、１０００万ドル以上がアルゼンチン等からロシア、スイス等に送金された。
１９９５年、９６年	アルゼンチンのハッカーがアメリカ海軍研究所その他の国防総省施設、ＮＡＳＡ、ロスアラモス国立研究所のコンピューターシステムに侵入した。
１９９５年～９６年	極右とみられる組織が、４回にわたってイタリアの通信社、中央銀行等のコンピューターシステムに侵入し、システムをダウンさせたり脅迫的なメッセージを出現させたりした。
１９９６年	学生が、アメリカのプロバイダのコンピューターシステムに侵入し、顧客のクレジットカード番号を不正に入手し、３万ドルを支払わなければ公開する旨を告げて脅迫した。
１９９６年９月	スウェーデンのハッカーにより、アメリカ中央情報局(CIA)のホームページが改ざんされた。
１９９８年２月	アメリカ国防総省、教育機関、民間企業等のコンピューターシステムに対する大規模な侵入事案が発生した。
１９９９年５月	アメリカ連邦捜査局(FBI)のホームページサーバーが、アメリカ国内のハッカーに対して行った捜索に対する報復とみられるＤｏＳ攻撃を受け、サービス停止に追い込まれた。
２０００年２月	アメリカ大手商業サイトがＤｏＳ攻撃を受け、数時間に渡ってサービス停止に追い込まれた。