政策の名称	**１　厳しさを増す犯罪情勢に対応するための警察活動の強化** **（５）情報セキュリティ対策の推進** **・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、平成15年度において、サイバーテロ対策要員の能力向上研修を実施する。
必要性	**【公益性】** 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月及び13年８月に中央省庁等ホームページ改ざん事件が発生し、また、平成12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14年６月に高度情報通信ネットワーク社会推進戦略本部が決定したe-Japan重点計画-2002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。 **【官民の役割分担】** サイバーテロは、一旦発生すれば重大な被害が発生し、国家又は社会の重要な基盤が機能不全に陥るおそれがあるため、その未然防止及び事案発生時における的確な対処を図ることは、公共の安全と秩序の維持を担う警察の責務である。 **【国と地方の役割分担】** 警備活動に必要な経費及び国の公安を害するおそれのある犯罪の捜査に必要な経費については、国庫が支弁することとされている。 **【民営化・外部委託の可否】** 本研修は民間の専門研修機関に委託し実施するものである。 **【緊急性の有無】** 重要インフラ関連サービス活動の多くが、情報システムにますます依存するようになってきており、今後、更に加速的な情報化・ネットワーク化の進展が見込まれる中、サイバーテロの脅威はますます高まっており、その未然防止及び事案発生時における的確な対処のために、喫緊に所要の対策を講じていく必要がある。 **【他の類似政策】** なし。 **【社会情勢の変化を受けた、廃止、休止の可否】** 重要インフラ関連サービス活動の多くが、情報システムにますます依存するようになってきており、今後、更に加速的な情報化・ネットワーク化の進展が見込まれる中、サイバーテロの脅威はますます高まってきており、今後とも、一層強力に対策を講じていく必要がある。
達成効果等	**【今後見込まれる効果】** 平成15年度予算により上記の施策を講じることができれば、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を図ることができる。 （参考）平成13年度における研修の実施効果 平成14年５月～６月の2002年ワールドカップサッカー大会の開催に際しては、研修を受けた各都道府県警察のサイバーテロ対策要員を含む警察官がサイバーフォース要員等と連携し、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、大会関連の施設や重要インフラ事業者等442団体の管理者対策を実施し、サイバーテロを完全に封圧した。 **【効果の発現が見込まれる時期】**

	研修終了時。		
予算額	**【平成15年度要求額】**　　30,438千円		
効率性	【代替的手段の有無】 サイバーテロは、一旦発生すれば重大な被害が発生し、国家又は社会の重要な基盤が機能不全に陥るおそれがあるため、その未然防止及び事案発生時における的確な対処を図るためには、サイバーテロ対策要員の能力向上が不可欠であり、代替的手段はない。 **【他の事業との連携】** サイバーテロ対策要員の育成、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・分析能力の向上、重要インフラとの連携の一層の強化を図ることにより、サイバーテロの未然防止及び対処をより確実に行うことができる。 **【効果とコストとの関係についての分析】** 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教養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。		
学識経験を有する者の知見の活用	なし。		
その他			
政策所管課	警備企画課	評価実施時期	平成１４年８月

平成１４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１３年１月１日～平成１３年１２月３１日）

○　不正アクセス行為の認知件数　１，２５３件

・　ホームページの改ざん、消去を伴うもの　　９３５件

・　ＤＤｏＳ用攻撃ツール（注）が仕掛けられていたもの　１７８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１３年１月１日～平成１３年１２月３１日）

○　コンピュータ不正アクセス被害届出件数　５５０件

・　権限取得行為（侵入行為）　　９７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１３年１月１日～平成１３年１２月３１日）

○　届出のあった不正アクセス関連行為　　２，８５３件

・　システムへの侵入　　１０３件

・　サービス不能攻撃　　６６件

（注）DDoS 攻撃とは、インターネット上の複数のコンピュータに DoS 攻撃（標的となるサーバに過剰な負荷をかけるなどして当該サーバのサービスを妨害する攻撃）用のツールを仕掛け、攻撃者の使用するコンピュータからの命令により一斉に DoS 攻撃を行い、標的となるサーバのサービスを妨害するものである。

DDoS 攻撃ツールが仕掛けられていた場合は、オペレーティングシステムの再インストールにより攻撃用ツールを削除するとともに、オペレーティングシステム及びアプリケーション・プログラムのバージョンアップ並びに定期的点検等により再発に注意しなければならない。