4．「連邦進入探知ネットワーク（FEDNet）」

- これまで連邦省庁内には、すでに独自のネットワーク防衛システムが導入されている。特に国防総省にはJTF-CNDという軍事関連システムを一括監視するシステムが存在しているが、省庁を横断するセキュリティは脆弱、各省長官の情報共有も進んでいない。
- FIDNetは、JTF-CNDに類似するものを、国防総省以外の省庁ネットワークに適用しようというもの。それにより、連邦省庁における攻撃、進入検知を自動化し、ひとまとめにしたい。少ない人材で、各省庁に平均的なセキュリティを提供することを目指す。
  R&D予算として1,000万ドル（大統領要求）。

3．米国におけるサイバー犯罪への取組における問題点

（1）組織体制における問題点

米国におけるサイバー犯罪への対応は国の機関が中心であり、国の機関でも特に組織上はFBIが主導しているNIPCが中心となっている。しかし、その体制構造は図2に示したように非常に複雑かつまとまりがない状態と言っても過言ではなく、各機関からもその組織体制の脆弱性、対応能力の欠如が指摘されている。

特に、NIPCは「いかなる機関がデータを共有していようと、すべての情報に対する権利を要求し、すべての情報を法執行力に分類して、殆どの諸機関自らが支援する業界と同情報を共有できない」ようにしたため、各政府機関で問題となり、NIPCは殆どの情報をすべての関連諸機関と共有できなくなる状況となっている。2000年2月の時点で36政府諸機関のうち6機関を除くすべての機関がNIPCに対する支援を中止した。シークレットサービス、CIA（中央情報局）、NSA、DIA（国防省国防情報局）は非公式な同盟を結び、NIPCを経由しないで情報交換を行っている。

（2）官民協力における問題点

民間企業においては、情報自由法（FOLA）に起因する情報のプライバシーの保護が最大の問題となっている。官民協力による情報共有機関はInfraGard、NSTACなど各種あるが、外部への漏洩という潜在的な懸念を常に抱えている。

情報自由法（FOIA）： 政府に保管されている殆どの情報について、市民の要求に応じて公開することを義務付けるもの。機密情報、軍事情報、個人情報、FBIの事件ファイルなどの例外はある。企業が政府と共有した情報については、法的に非公開とすることは出来ない。

（3）予算関連の問題点

連邦政府は情報セキュリティのための十分な予算を確保できていないのが現状である。議会が個別の政府機関に対して情報セキュリティ対策費として内容を十分に吟味することがないため、多額の予算を割り当てることはなく、連邦省庁の情報セキュリティ対策費を一括し、連邦政府全体としてのセキュリティ対策予算としている。この一括した予算を各省庁が担当する13の小委員会を通じて省庁別に予算配分している。

このため、議会には各省庁で行われている情報セキュリティプログラムをまとめて吟味し、予算配分を行うというメカニズムが存在しない。特に省庁横断型の情報セキュリティプログラムには予算、人員とも十分な割り当てが与えられない。このため、他のセキュリティ機関との適切なコミュニケーションがとれず、各省庁の活動が必ずしも統一性のあるものにはなりえないことが問題として指摘されている。