

米国におけるサイバーテロ対策状況調査報告

The status report on the US preparation for measures against cyber terrorism

Douglas Webb*1, Edward Blackwell*2, 門野健治*3

dwebb@atomic Tangerine.com, eblackwell@atomic Tangerine.com, kkadono@sri.co.jp,

*1, *2 AtomicTangerine Inc. *3 アトミック・タンジェリン株式会社

現代社会の基盤である、情報通信、金融決済、電力、交通、石油・ガス、水道、緊急サービス（民間のサービス及び警察・消防等）、政府サービスなどの分野で、それぞれの情報システムが攻撃を受け、破壊ないし機能停止などに陥った場合の被害は甚大であり、重要な社会インフラを守ることは、国家の安全保障の面からも必要不可欠となりつつある。1997年、米国では重要インフラ産業に対して、その情報システムを外部の攻撃から守るべく準備するようという要請が、大統領令63号（以下 PDD63）として発令され、それに従って各産業界でセキュリティ対策が推進されてきた。本報告は、米国の政府機関および民間企業がどのように PDD63 に対応しているのかについて、1999年9月～2000年2月の間に行なった調査プロジェクトの結果をまとめたものである。

1. はじめに

本報告は、SRI コンサルティング（アトミックタンジェリンの情報セキュリティ部門の前身、以下 SRIC とする）が、情報処理振興事業協会（以下 IPA とする）からの依頼に基づいて行った調査プロジェクトの結果を提供するものである。この調査は、米国大統領令 63 号（Presidential Decision Directive 63: PDD63 と略される）に対して、米国の政府機関および民間企業がどのように対応しているのかについて行なったものである。PDD63 は、米国の重要インフラの保護に関するもので、特に、通信や金融等の分野（セクター）を特定して、対応を推進しようとするものである。

本プロジェクトにおいて、重要インフラの保護および PDD63 に関連する情報およびドキュメントを収集し（PDD63 の文書本文は秘密扱いとなっている）、また電話や面会によって、対象となる各セクターの代表者に対するインタビューを実施し、それらを評価/分析し、まとめた。

2. 米国における重要インフラの保護政策 (PDD-63)

2.1 PDD63 が発令された背景

今日、米国は、軍事的には圧倒的な強さを持っているため、将来の米国の敵となる国家、グループあるいは個人が、従来の方法以外の方法で米国を攻撃しようとする恐れがある。米国経済は、情報通信システムによって支えられたインフラにますます依存するようになってきており、イン

フラや情報システムに対する、非従来の攻撃が、米国の軍事的および経済的に大きな被害をおよぼすことができるようになりつつある。

上記の重要インフラとしては、経済や政府の運営の効率化に欠かすことのできない物理インフラと情報通信システムの双方を含んでいる。その主要なものとしては、政府や民間による通信、エネルギー、金融、運輸、水道システム、緊急サービスなどが挙げられる。これらのシステムの多くは、物理的にも論理的にも歴史的にそれぞれ独立しており、従来は相互に依存関係はなかった。しかし、情報技術の進歩と効率改善の要請によって、これらのインフラの自動化や相互接続が行われるケースが増えてきている。一方で、こうした進歩は、装置の故障、人間によるミス、天災等自然災害、物理的なあるいは情報システムを通じた攻撃など、新しい形のシステムの脆弱性をもたらしている。このような脆弱性に対処するためには、公的部門と民間との両者にまたがる、柔軟で段階的なアプローチが必要となる。

2.2 大統領による PDD63 発令の意図

米国では重要インフラの持続性、頑強性を確保することが政策として行われてきた。クリントン大統領は、情報システムを含む重要インフラに対する、物理的および情報ネットワークを通じた攻撃に対する脆弱性を迅速に排除するため、全ての手段を講じることを意図して、PDD63 を発令した。

2.3 米国の目標

米国は 2000 年までに初期段階の運用能力を達成し、大統領がこの大統領令に署名して5年以内（2003年）に、以下のようなことを目的とする意図的な攻撃行為から、国家の重要インフラを防御する能力を獲得、維持することを目標としている。

- 必要不可欠な国家安全保障のミッションの実行や、一般の人々の健康や安全を守るといふ、国家の能力を低下させる行為
- 秩序を維持し、最小限の基礎的な公的サービスを提供するという、州政府や地方政府の能力を低下させる行為
- 経済の秩序ある機能、通信、エネルギー、金融、運輸などの基礎的サービスを提供する民間セクターの能力を低下させる行為

2.4 脆弱性の低減のための官民の協力関係

重要インフラ攻撃のターゲットには、民間と政府の双方の施設が含まれるため、潜在的な脆弱性を排除するには官民双方の密接な共同作業が必要となる。成功の鍵は、真の相互の協力関係にある。PDD63では、重要インフラの脆弱性を排除するという国家目標を達成するため、民間セクターに対して、政府の規制を強化することや、予算の手当てなく強制措置を広げることを極力排除するべきであるとしている。

PDD63によると、インフラ攻撃による影響を受け易いと考えられる主要なセクター（業界）の各々について、連邦政府は指定したリード・エージェンシー（Lead Agency）から、その上級職員をセクター・リエゾン・オフィシャル（Sector Liaison Official）に指名し、民間セクターと共同作業行わせる。インフラに関連する民間セクターとの議論や調整を行った後、セクター・リエゾン・オフィシャルは、各業界を代表する民間側の相手としてセクター・コーディネータを決定する。

この2名と各々が代表する国の部門あるいは企業は、各セクターの国家インフラ保障プラン（National Infrastructure Assurance Plan）づくりのために、以下の協力を行う。

- サイバー・アタックおよび物理的攻撃に対するそのセクターの脆弱性の評価を行う
- 重大な脆弱性を除去するための計画を推奨する
- 主要な攻撃を発見し予防するためのシステムを提

案する

- 発生中の攻撃に対して、警報、抑制、拒絶するための計画を作成し、必要に応じて、連邦危機管理局（FEMA）と連携して攻撃の影響に対応するため、最低限の基本的な機能を迅速に再構築する

セクターごとの計画を作成する際には、ナショナル・コーディネータは、リード・エージェンシーのセクター・リエゾン・オフィシャルおよび、国家経済審議会（National Economic Council）の代表とともに、インフラ・システム間の相互依存性に特に焦点を当てながら、各セクターのプランの全体的な調整と統合を行う。

2.5 ガイドライン

これらの潜在的な脆弱性とそれを除去する方法に取り組むため、クリントン大統領はこれら関係者に対して以下のような原則と留意点に気をつけるように指示している。

- 大統領令に記された目的を達成するために、その方法とプログラムについて議会に相談し、議会からの意見を聞くこと。
- 重要インフラの保護は、インフラ所有者、運用者、政府の間の共通の協力関係と責任の基に行われるべきである。さらに、連邦政府はこの世界的になりつつある問題について、国際的な協力を推進する。
- 重要インフラに対する脅威となる技術や脅威の性質は、非常に速く変化し続けているので、重要インフラの信頼性、脆弱性、脅威となる環境については、随時評価をし続ける必要がある。
- マーケットからのインセンティブを与えることによって、重要インフラの問題への対応を促すべきである。また、規制は最低限とすることとする。
- 重要インフラの保護を達成、維持するために、必要に応じて警察、規制、諜報、国防等の政府の機関、機能、リソースを使用することができる。
- プライバシーの権利を尊重し、情報は正確に、機密に、安全に取り扱われなければならない。
- 連邦政府は、研究開発と資機材調達との両面で、インフラ保護機能の導入を推進する。
- 連邦政府は、民間セクターに対するインフラ保護のモデルとなる。
- 危機管理だけではなく予防も対象とする。このため、民間側は必要な安全性を確保することと、政府に必要な情報を提供することが求められている。

インフラの所有者と運用者は、自発的に参加する

この会議は、安全保障、インフラ保護および対テロリ

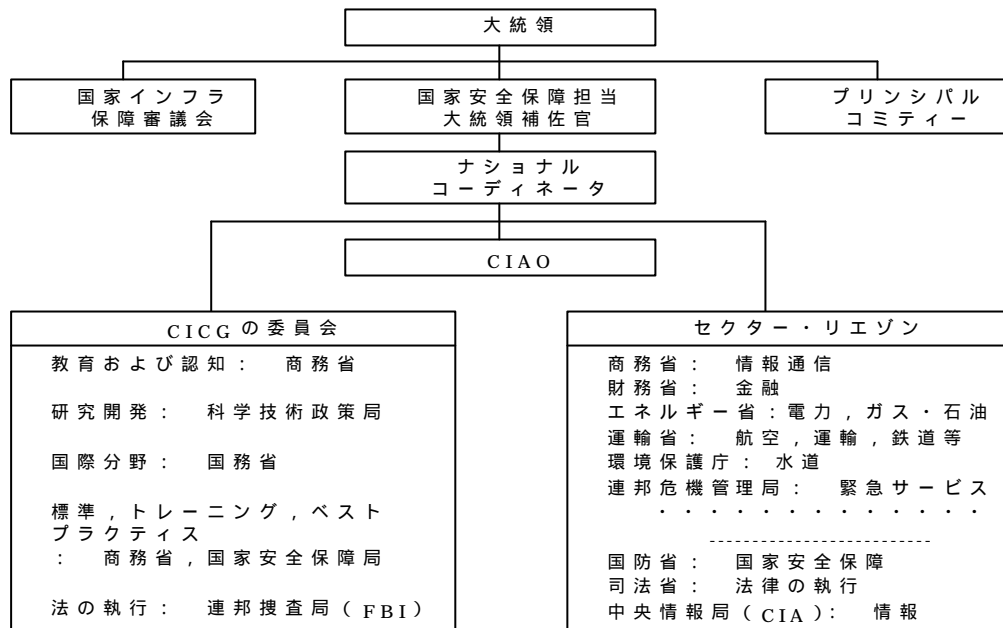


図 1 . 米国の PDD63 推進組織体制

ことが望ましいとしている。

- 全ての重要インフラ保護の計画と実行は、州政府、地方政府に配慮し協力して行われる必要がある。

2.6 組織構成

連邦政府は、この目的のために4つの構成要素で構成される(図1.米国のPDD63推進組織体制)

● セクターの連絡のためのリード・エージェンシー

攻撃を受ける恐れがある各々の重要インフラについて、連絡のためのリード・エージェンシーとなる政府部門が決定され、アシスタント・セクレタリー・レベルかその上位の者を、セクター・リエゾン・オフィシャルとして任命し、民間の代表であるセクター・コーディネータと共同で問題に当らせる。

● 個別機能ごとのリード・エージェンシー

重要インフラ保護の機能分野ごとに、リードエージェンシーを決定しその分野における全ての活動の調整に責任をもつものとする。

● リード・エージェンシー間の協力

セクター・リエゾン・オフィシャルと各リード・エージェンシーのファンクショナル・コーディネータは、国家経済審議会(National Economic Council), 政府の関連機関、関連部門などからの代表者ととも、大統領令を具体化するための調整を行う会議を開催する。

ズム対策のナショナル・コーディネータ(The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism)が議長を勤めるCICG(Critical Infrastructure Coordination Group)が支援を行っている。このナショナル・コーディネータは、国家安全保障担当補佐官を介して大統領の指揮下にある。

● 国家インフラ保障審議会(National Infrastructure Assurance Council)

リード・エージェンシーの推薦により、国家経済審議会(National Economic Council), ナショナル・コーディネータ, 大統領は、国家インフラ保障審議会(National Infrastructure Assurance Council)として、主要なインフラ・プロバイダー, 州政府, 地方政府からなるパネルを設置する。この審議会において、議長は大統領が指名し、ナショナル・コーディネータは、審議会のエグゼクティブ・ディレクターとして参加する。審議会はインフラ保護の分野での官民の協力を促進するために、定期的にかかれることになっており、また、必要に応じて大統領に報告書を提出する。

2.7 連邦政府のインフラ保護

国家の重要インフラを所有している政府の各部門は、各々

がそのインフラを保護するための責任を負っている。そして、各政府関係機関の最高情報担当責任者（CIO）は、その情報の安全を確保する責任を負う。これに加え、各政府部門と政府機関はそれぞれ、最高インフラ保護担当責任者（Chief Infrastructure Assurance Officer: CIAO）を、インフラ保護の役目に当らせるために任命する。CIAOはCIOと兼務になる場合もある。これらの担当責任者は、政府のコンピュータや物理システムに対して実施する脆弱性評価を行うための正当な手続きを確立することになっている。

また、大統領令の発行後 180 日以内に、全ての政府部門および機関は、その保有する重要インフラを保護するためのプランを策定することが義務付けられている。政府の部門相互間にまたがるような問題の分析には、ナショナル・コーディネータが調整に当る。また、CICG は専門家の立場からレビューを実施する。大統領令発令から 2 年以内に、これらのプランは実行に移され、2 年おきに更新されることとなっている。これらによって、連邦政府は民間企業に対して、インフラの保護を実施するための最良のモデルを提示する。

2.8 National Infrastructure Protection Center (NIPC)

NIPC は、1998 年 2 月に米国司法省と FBI により、ワシントンにある FBI の本部内に設立された組織である。このセンターは、政府と民間セクターとの共同によるもので、政府の関連機関、連邦政府、州政府、地方政府および民間セクターから代表者が派遣されている。NIPC は、PDD63 のフレームワークの一部を構成するもので、重要インフラに対する攻撃による脅威の評価、警告、調査、対応についての全米のフォーカス・ポイントとして機能するものである。この組織のミッションのなかで、重要なものとして、政府とインフラを所有ないし運用する民間との間で、システムの脆弱性や脅威に関する情報を共有化するメカニズムを構築することが含まれている。

2.9 Information Sharing and Analysis Center (ISAC)

民間セクターが情報を共有、分析するためのセンターである。ナショナル・コーディネータが、セクターの連絡担当者や国家経済審議会（National Economic Council）とともに、民間のインフラ所有者、運営者に強く設立を働きかけることとなっている。このセンターの実際の機能やNIPCとの関係は、連邦政府の助言を得て民間セクターが決定する。大統領令の発行後、180 日以内にナショナル・コーディネータは国家経済審議会（National Economic Council）

を含む CICG の支援を受けて、ISAC の設立を促進する支援策を決定することとなっている。

このセンターは、民間セクターの情報を収集、分析し、差し障りのある部分を削除し、その民間セクターの情報を業界や NIPC に提供する。また、NIPC から情報を収集、分析し、さらに民間セクターへ配付するということも行う。現在、ISAC は金融セクターと電力セクターで設置されている。

2.10 InfraGard

NIPC の情報共有化活動の中で重要な位置を占めているのが InfraGard である。このプログラムは、1997 年にクリーブランド（Cleveland）でのパイロット・プログラムとして開始され、少なくとも全米の主要都市に拡張される予定である。このプログラムは、情報システムへの侵入、システムの脆弱性について情報を双方向に共有化するメカニズムを構築しようとするものであり、その目的は以下のようになっている。

- メンバーに対する、インフラの脆弱性やその防御法についての訓練および教育のためのフォーラム提供
- メンバーに対する、迅速で付加価値の高い、危険性の通報、警報および警告
- InfraGard メンバー、FBI の地域オフィス、NIPC などの間で共有化されたコンピュータへの侵入 / 攻撃情報の保護を確実にすること
- FBI の地域オフィスや NIPC に提供される侵入 / 攻撃情報を質、量ともに充実すること
- InfraGard のメンバー、FBI の地域オフィス、NIPC などの間で、インフラへの脅威、脆弱性、相互依存性などについての相互交流や情報の共有化を活性化すること

InfraGard のプログラムのメンバーは、次の 4 つの基本的なサービスを利用することができる。

- InfraGard の地域部会への参加
- サイバー・アタックの情報を自動的に知らせるアラート・ネットワークへのアクセス
- 最新のインフラ保護に関する情報を掲載した InfraGard のウェブサイトへのアクセス
- NIPC に設置されたヘルプデスクの活用

3. 米国政府および産業界の重要インフラ保護への取組み

3.1 インタビュー調査の実施

PDD63 に直接関わっている人物からの情報を入手することを目的として、米国の政府関係機関および民間企業に対してインタビュー調査を実施した。インタビュー対象は、PDD63 に関わっている人々から代表的なサンプルをバランスを考慮して選定した。ただし、インタビュー調査という性格上、サンプル数には限りがあり、以下に述べることが必ずしも米国政府や産業界の平均的動向であるとは言えない場合がありえる。また、業界ごとの議論においても、インタビュー先が必ずしも全業界を代表しているとは言えない可能性がある。

インタビュー先としては、PDD63 で重要インフラとなっている 8 つの産業セクター（通信、電力、ガスおよび石油の輸送および備蓄、金融、交通・運輸、水道、緊急サービス、政府サービス）について、それぞれ数件づつを選定した。これらには、各分野の主要な企業が含まれている。

3.2 調査結果の構成

調査の結果は次のセクションにて詳述することとする。以下は、本調査で重点を置いている重要な課題と問題に関連する 7 つのサブセクションとなっている。

- 官民協力
- 資源（特に人的資源）の投入
- 施策
- 政策に関連した情報セキュリティの重要性認識
- 民間企業の PDD63 への対応
- サイバーテロの実例
- 企業内での PDD63 に関する教育

なお、本報告では個別の企業名、機関名が特定できる情報は削除しており、該当する項目についての一般的な動向としてまとめている。インタビューを円滑に実施するためにも、そのような匿名性を保証することが必要であった。

3.3 官民協力

3.3.1 概論

PDD63 に基づく重要インフラの保護への対応では、対応を義務づけられている政府の部門や関係機関（エージェンシー）と、実際に自らのインフラ保護に責任を負ってきた民間の事業会社との対応に違いがある。一般に、米国においては民間企業は政府からの強い独立心を持っており、政府が民間分野に関与することを嫌う傾向にある。また、政府が旗を振ったからといって、自社にとっての便益が見えない限り簡単には協力しない。本調査において発見された主要な課題は、(1)情報の共有化をいかに推進するか、と

いう点と、(2)だれが PDD63 に基づいて行うインフラ保護策のために必要となるコストを賄うのか、という点である。

一方、PDD63 の最も大きな成果とみられるのは、それぞれの産業セクター間、あるいは、産業セクター内の各機能の間、政府と産業界の間等の相互依存性に着眼しこの問題を取り扱ったことである。

情報共有の点については、多様な参加者が存在しその各々の間に複雑な関係があることなどのために、相互に全面的に協力することは難しくなっている。政府関係機関の間でさえ、相互に情報を提供しようとはしない傾向がある。ただし、意識の上では少なくとも最小限のレベルでインフラを保護するために協力することの重要性は認識されている。また、経済界と政府とが相互に依存していることも認識されている。

PDD63 を支えるにあたって、政府機関には 2 つの極めて重要な問題点がある。第一に、PDD63 に対するコンプライアンス（規定への準拠）を調整する責任は、ナショナル・コーディネータと CIGC に付与されている。しかしながら、それらは大統領令を実行するうえでの権威や、現実的な統制メカニズムを持っていないように見えることである。また、第二には、PDD63 には、CIGC やリード・エージェンシーが大統領令に従うための財政的な支援がほとんどないことである。

大統領令の定める必要事項を満足するために、政府関係機関の多くは適切な措置を講じようとしてきた。しかし、そのほとんどは大統領令に定められた 2000 年 5 月の実行期限に完全に間に合わせることはできなかったと見られる。その原因は、これら政府機関において必要となる予算や人員が十分に確保できないことと、政府自身のシステムについて必要となる作業量が過小に評価されていたと見られることである。政府にとってより理にかなった効率的なアプローチは、関係機関が保有するインフラシステムへの損害を最小限に止めることを目的として、システムへの攻撃を発見し対応策をとるための運用プランを作ることであったと思われる。

3.3.2 情報共有の問題点

今回実施したインタビューでは、ほぼ全ての人が民間企業側の情報を政府と共有することの問題点について言及した。すなわち、情報のプライバシーが守れるかという問題と、その情報が意図しない別の用途に使われないかという問題である。前者の問題点は、後述する情報自由法（FOIA）に起因する問題であり、後者は連邦捜査局（FBI）などに

提供した情報を流用されないかという懸念である。PDD63が現実に効力を発揮するためには、これらについての何らかの解決策が必要である。

さらに一般的な疑問点としては、どのようにしたら共有化される情報が保護できるかという点が挙げられる。より多くの人々が情報に接することが可能となれば、より情報が漏えいする危険性が高まることとなる。さらに、ただ単にリストや情報を集積したものを持っているだけでも、犯罪者にとっての魅力は増大し、情報が漏れた場合の損害も大きくなる。また、協同的な環境では、共有化された情報に対して何かが発生した場合の法的責任の問題も発生する。

以下は、インタビューからの引用である。

- ✓ 私達は、そのことが顧客にとって有益であり、……
そうしたことが起こらないと予測されるならば、確実に情報の共有を行うだろう。
- ✓ 政府のインターネットのセキュリティに対する役割は、未だよく定義されていない。

3.3.3 情報自由法 (FOIA: Freedom of Information Act)

情報自由法は、政府に保管されているほとんどの情報について、市民の要求に応じて公開することを義務づけるものである。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があり、公開の対象として全ての情報が含まれるというわけではないが、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できない。そのため、政府を通じて情報の共有化を図ろうとする企業は、ジレンマに陥ることとなる。

3.3.4 InfraGard におけるFBI の役割

大統領令は、インフラ保護のための調整業務を FBI 配下の National Infrastructure Protection Center (NIPC) に割り当てている。政府と民間企業間、および、民間企業どうしの間での協力関係構築を推進する主要な推進力となっているのは、InfraGardの設置であった。

InfraGardは、FBIをスポンサーとし、企業、研究機関、政府関係機関からなる組織であるが、法的に、及び、財政的に政府のコントロール下から独立しているとされている。その目的は、基礎的インフラの保護に関する情報の交換である。この機関は、システムへの攻撃や情報漏洩に関して、問題点を共有し自主的に他のメンバーや FBI に情報を提供するフォーラムを主催する。あるインタビューでは、論理的なセキュリティやインターネット・セキュリティの専門性が不足しているのではないかと見ている。

この機関のもうひとつの役割として、参加企業が共有したいと考えるシステムへの攻撃に関する情報のデータベースを、構築・維持することが挙げられる。しかし、ここで提供された情報が、FOIAのために外部に公開されるといふ潜在的な問題点がある。場合によっては、そのような調査の結果が、情報提供者に対しての犯罪につながる恐れもある。

3.3.5 民間側の情報共有に対する態度

インタビュー調査の結果では、情報の共有に関する各社の態度はそれぞれ非常に異なっている。いくつかの企業は実際に NIPC との間で情報の共有を行っているものの、ほとんどの企業は情報の共有に全く消極的である。あるインタビューでは、法的に要求されないかぎりインフラに対する攻撃などの情報を一切共有しないことが強調された。FBI、顧客、従業員等と、そのような事例に関する情報を共有したり、限られたメンバーに対してでも簡単な報告を行う企業は極めて少い。インタビュー調査において、PDD63が発令された結果によって、情報の共有化において何らかの変化があったか否かについて尋ねると、ほとんどの回答は「少なくともまだそのような変化はない。」というものであった。

ほとんどの企業にとって何を共有化するか選定するうえでジレンマがある。仮に何もそのような情報を共有しなければ、従業員（あるいは関心をもつであろう人々）が、危険の存在を認識しない可能性がある。もし、あまりに多くの情報を共有した場合には、損害をもたらすかも知れない犯罪者に対して動機づけを与えてしまうかも知れない。現在のもっとも一般的な情報共有の形態は、相互に信頼がある個人間での情報共有である。この場合、情報を公開された個人は、その情報を活用するかも知れないが、その情報の出所や具体的なことについては特定されないようにしている。

3.3.6 Y2K モデル

米国政府では、コンピュータ 2000 年問題 (Y2K) での政府と産業界との協力関係が、インフラ保護のための知見となり、一つの優れたモデルになり得ると考えている人々がいる。Y2K 問題への対応は、ほとんどの政府及び産業界の人々にとって成功であったと考えられている。このことは、適切な環境が整えられれば、政府の関係機関は相互に協同作業を行うことができること、そして、産業界が政府と一つのチームとなって協同作業を行うことができること

を示している。

このモデルが機能するために、議会や政府の要人、産業界のリーダーなどが率先して、推進力とならなければならない。言い換えれば、議会がそのような活動を後押しし、大統領と主要な企業の CEO がそれを積極的に支援しなくてはならない。

しかしながら、インフラの保護と Y2K 問題の対応とではいくつかの点で大きな違いがある。

- Y2K 問題では、1000 億ドルにも及ぶとみられるコストがかかった。インフラに必要な資金は、確固とした見積もりが行われていないために、さらに巨額なものとなるとみられる。
- Y2K 問題は協力のレベルと情報共有のレベルにおいて独特であった。問題の緊急性のために、通常よりも非常に高いレベルで情報の公開が行われた。コンピュータ・セキュリティの設計に関する情報には、広範囲にアクセスすることができた。
- Y2K 問題は、インフラの保護に関する種々の問題と比べて相対的に焦点を絞り易かった。世界的な視点にたって見た場合、インフラ保護について何をを行うべきかという評価のためには、複雑なリスクアセスメントが必要となる。リスクアセスメントは、正確な科学ではないため、どの程度の費用を費やすべきかについて、あるいはそのような危険性を正すことにさえ、同意しない人々がいることは理解できる。
- Y2K 問題には、絶対的な期限があった。インフラの保護に関しては、リスク要素の評価によって、問題点が解決されるまでその組織は十分な時間対応を先送りすることができる。

インフラ保護に関する協力関係の構築は、Y2K 問題の場合の数倍大きな問題である。ある政府関係者曰く、「将来は流動的である。」

3.4 資源（特に人的資源）の投入

少なくとも人的資源についてみると、PDD63 を推進するために政府は非常に大きな投資をしている。政府は、専門委員会や市民による委員会を設置し、多くの懸念される問題点に取り組んでいる。一方、これに対して産業界側では PDD63 を支援する目的で、割り当てたリソースは比較的少なかった。産業界側が提供した主だったリソースとしては、上記のような委員会活動に対する幹部社員の派遣と、セキュリティの専門スタッフの InfraGard の作業への派遣

である。

3.4.1 誰がコストを負担すべきか？

今回のインタビューにおいて、政府に属する人々のうち数人が、政府は少なくともこれまでのところ必要なコストのうち主要な部分を負担してきたと感じていることが分かった。しかし、あるコスト見積もりによるとこれまでのコスト負担は、75%が民間側であり、政府の負担は 25%となっている。このことは、政府は資金的な負担よりもむしろリーダーシップの面で貢献していることを示している。協力関係が機能するためには、資金的な裏づけが必要となっている。現在のところ、自分のことは自分で解決せよという風潮があり、すなわち、自社内での問題があった場合には自分の資金で解決しなければならないということになっている。

クリントン大統領は 2000 年始めのスピーチの中でコンピュータへの攻撃に対して相当額の資金を割り当てることを提案した。この資金は、ハッカーからテロリストまでの広範な脅威に対抗するための長期計画の一部となるものである。そのスピーチの中では直接的な言及はしなかったものの、PDD63 の言葉遣いと極めて近い表現が使われている。

3.4.2 産業セクターによる違い

産業分野やセクターの中には、脅威の度合いが高いためにより多くのリソースを割くことが必要となるものがある。セクターの中には影響を他者に波及させやすいものがある。特に、電気通信分野に対しては他のすべてのセクターが、依存している。例えば、あるインタビュー先は、次のように言っている。「我々は、米国における鉄道を高速道路や空港と比較することができる。代わりとなる道路や近くに別の空港があるために、一つの高速道路や空港に対する被害は、交通の流れに対してはあまり大きな影響を与えない。一方、鉄道の車両運行は集中制御が行われている。もし、鉄道をつなぐ音声やデータの通信が失われると、鉄道のシステム全体がすぐに混乱に陥ることになる。」

民間企業のほとんどのインタビュー先は、PDD63 によって特に変わったことはしていないと言っている。

- ✓ 適切かつ慎重なセキュリティの方法を検討したうえで、それ以上にセキュリティに資源を費やすことはしない。
- ✓ 我々は情報セキュリティに相当の労力を費やしているが、PDD63 には直接関連していない。

一方、あるインターネット・サービス・プロバイダーは、次のように言っている。「我々はセキュリティを非常に重要であると考えている。PDD63 は、我々の情報セキュリティに対する対応のわずか一部である。情報の共有化はセキュリティを改善するための鍵となる。我々は、顧客がそれを禁じない限り、そのような情報共有を行う。しかし、その場合でも問題点は一般的なことばで表現され共有されることになる。」

明確なコストとして言及されたのは、InfraGard の活動に関連するものである。しかし、例外として InfraGard を強力に支援するなど、PDD-63 関連の活動に相当の企業リソースを割いている例があった。結論として、現在だれもどのように資金を調達するか良い答えを持ち合わせていないと言える。

3.5 施策

3.5.1 政策の促進

現在、InfraGard における活動以外に、NSC や FEMA などいくつかの鍵となる政府機関において、インフラ構成要素に対して責任を有する人々の支援を得るために、強力な促進策が講じられている。産業界は、主として自社固有の情報や慎重な取り扱いを擁する情報を守ろうと考えているため、この活動を強力に押し進めることに対して躊躇を感じている。

InfraGard 以外の産業界の活動はこれまでそれほど成果を上げていない。意欲的な取組みが行われ、ある程度の成果が出ているものの、産業界やセクターごとで一貫性は見られず、非常に強力に推進している企業がある一方で、ほとんどの企業の取組みは非常に少ないのが現状である。その産業界の抱えている関心よりも、特定の個人レベルが持っている関心の方が重要となっている。

3.5.2 施策による成果

いくつかの例外を除いて、今回のインタビューを受けた人々は、この活動は国家全体および彼等が属する企業、行政機関などにとって極めて有益であるという点で一致している。PDD63 への対応は、既に完成したのではなく現在進行中のものであるため、発生しているいくつかの問題点についてその深刻さや予想される解決方法について論じるには、まだ早すぎるものと見られる。仮に情報を共有化することの問題点が解決されるならば、資金面の問題は解決できるだろうという楽観的な見方がある。

国際的には、他国と情報を共有化することに躊躇があり、

特に、国家利益の保護の問題があるところでは特にその傾向が高い。銀行、水道、電力および通信などの主要インフラ産業の外国企業による所有も、もう一つの問題点を提起するものである。

運輸などいくつかの産業分野では、強制的な業界の運用標準が存在し、米国運輸省などによって管理されている。しかし、ほとんどの産業界ではそのようなことは行っておらず、それどころか、多くの産業で政府が産業界に関与することについては強い拒否感がある。このことは特に、インターネットに関連するような新しい産業にあてはまることである。

情報自由法 (FOIA) は、民間企業における問題点が公開されないよう改正される必要があるとみられる。しかし、今回のインタビュー先は、議会が本法の内容を緩和したり変更を可能とするための改定を加える可能性はまずないと見ている。政府の所有する情報の一般への公開、個人のプライバシーの権利、政治などで解決すべき問題点がいくつもあるためである。さらに、2000 年は選挙の年であるため、そのような議論を呼ぶような問題を提起することは、ほとんどあり得なかったとみられる。

PDD63 に基づくものではないが、慎重な取り扱いを擁する情報について、ある程度広範囲に、しかし制限された範囲内で情報を共有している例をいくつか挙げるができる。

米国 AtomicTangerine 社の実施している International Information Integrity Institute (I-4) プログラム (SRIC から移管) は、限定された会員組織で、すべてのメンバーは同じような専門的立場にあり、その全メンバーは秘密保持契約書にサインをする。メンバー間には高いレベルでの信頼感が存在し、メンバー内のみで情報セキュリティが破られた経験について情報を共有する。このプログラムには、政府関係機関のメンバーも参加しているが、彼等もまた秘密保持契約にサインをしており、ここで入手した情報をその所属する政府関係機関の事業において直接的に使用することも禁じられている。インフラやサイバーテロについて焦点をあてて、情報の共有をしているだろうと見られる情報セキュリティの機関はこの他にもいくつか見られる。

もう一つの事例として、National Security Telecommunication Advisory Committee (NSTAC) を挙げることができる。NSTAC は通信インフラを守るために、政府と産業界の協同のもと 20 の通信事業者が構成する機関である。NSTAC はワシントン D.C. 地域に位置し、メンバー企業の代表部をそのオフィスビルの中に置いている。こ

ここでは、日々の情報の共有化が図られ、継続的に緊急事態に対する対応準備を行っている。米国の司法長官は、重要インフラの保護に関することについてのみ、このグループに対する独占禁止法上の適用対象から除外することとしている。

金融業界では、政府関係機関の中で OCC(通貨監督局：Office of the Comptroller of the Currency)が最も影響力がある。この機関は、総ての金融機関について現行法令や手続きの遵守を検査する。OCC は2、3の監査報告書の中で PDD63 について言及しているが、具体的な指示はなく、また、監査内容とも関連づけて報告されているものはない。OCC の報告書(99-0 サイバーテロからのインフラに対する脅威)は、この問題を取り扱っている。

3.5.3 施策の問題点

FBI に対して PDD63 を実行するための責任が与えられている。FBI の中心的な使命は、捜査であり執行(強制)ではないため、この責務は少し通常と異なっている。(米国では、国家警察軍といったものが存在しない。そのような警察軍が存在すれば、彼等が PDD63 のような法律の内容を実現化するためのグループとして最も適している。)

PDD63 のそもそもの目的は、政府のインフラを保護することであったが、その実現化へ向けた活動が進むにつれて、政府のニーズと民間側のニーズとの境界が不明確となった。

FBI が関与していることと、もともとの大統領令の性質から、多くの民間の組織は参加に対して消極的である。以下は、民間側からのいくつかのコメントを集めたものである。

- ✓ マネージメントの人間と議論した結果、企業がターゲットとなるかもしれないと感じた。参加による便益は定量化することはできない。その結果、マネージメントは参加には用心した方が良いと感じた。
- ✓ 我々は参加を検討したが何らの行動も起こさなかった。我々は漠然とした認識を持っているが、知らぬは仏である。
- ✓ なぜ、民間が政府のこのリーダーシップを支援しなくてはならないのか？我々にはそこから得られるものはあるのか？別な言葉で言えば、参加することの費用対効果はどうなっているのか？
- ✓ これを経営者に理解させるのは難しいことだ。何が、これの利点や欠点となるのか？それが分から

ないので、これに参加することがより良いことにつながると経営者を説得するのは難しい。

- ✓ 企業は匿名性を求めているが、それはまだ保証されたわけではない。

多くの経営幹部は、政府に対して、自発的に提供された情報を保護するように、法律が変わらなければならないと考えている。

3.6 政策に関連した情報セキュリティの重要性認識

Y2K 問題はインフラの問題についての重要性の認識を高めたが、今日まで限定された範囲にとどまっている。同様に、投入されているリソースも限定されている。

そのような認識が欠如している例として、ある政府関係機関が挙げられる。この機関は、どのような結果をもたらすか考慮せずにインターネットに情報を掲載し始めた。その中には、米国内の数千の場所の脆弱性について詳述したものが含まれていた。これは、テロリストにとって攻撃目標を定めるための公開情報となりえるが、幸いなことに、実際には問題は起きなかった。

現在、産業界にはインフラの障害によって生じる「ドミノ」型の被害について、ほとんど認識がない。例えば通信ハブは、地域ごとに一地点に集約され世界的に配置されているが、これが、自然災害や外部からの攻撃によって破壊された場合、その地域に対する通信が1、2週間あるいは一ヶ月の間、実質的に存在しないのと同じ状態になる。同様に、ガスや石油のセクターにおいても、非常に重要度の高いパイプラインに冗長性がなく、大きな破損に対する平均修復時間の方が備蓄したものを利用できる時間より長くなるかもしれない。

もう一つの事例は、数年前にハリケーンがハワイ地域を襲ったときに、最大電力まで復旧するのに相当の困難を要したことが挙げられる。経験のある電力技術者や使用する電信柱が足りなかったことが、復旧時間に多大な影響を与えた。完全に復旧するためには、中心地から離れた地域では1年近くを要した。これらの例では、多くの主要インフラの障害によって発生する事故の連鎖の結果、経済的、社会的に大きな崩壊をもたらす可能性があることを示している。

PDD63 に関連して情報セキュリティについての認識を高める活動の中で重要な例の一つは、IIA(内部監査人協会：Institute of Internal Auditors)によるものである。IIA は、70,000 名の会員を有し、国際的な専門家によって構成される協会で、内部監査人やその組織に対して調査や教育、資

格、標準化、その他の活動を提供するサービスを行っている。IIA は情報のセキュリティと安全問題に対する認識を向上するための活動を行うため、米国の CIAO (Critical Infrastructure Assurance Office-大統領直属の委員会) と協力関係を結んでいる。IIA は、企業役員会向け情報セキュリティのリスク管理に関するガイドを用意し、情報セキュリティにおける監査者の役割について対話を開始し、次の3つを実施した。

- ✓ 取締役会のメンバーに対して、情報セキュリティの問題が事業に与える脅威についての認識を喚起し、情報リスクの管理を正しく行なえるようにするための報告書作成
- ✓ 情報セキュリティの問題に対応するため、産業界のリーダーや監査の専門家を集めて、2000年4月18日に行われたホワイトハウスにおける頂上会議(サミット)
- ✓ 上記のワシントンでの頂上会議(サミット)をもとに行われる、5つの地域会議

3.7 民間企業のPDD63への対応

概して、実際の脅威が存在するために、民間企業はPDD63の活動を支援している。しかし、通信や金融を除いて、委員会の仕事をするために幹部社員を派遣していること以外には、ほとんどの企業で経営資源をそのために割くことはあまり行われていない。以下は、PDD63への支援についてのインタビューで得られたコメントである。

- ✓ 我々は、米国の多くの都市で InfraGard に積極的に参加しており、NIPC および InfraGard に対してコンテンツを提供している。
- ✓ 技術面でも専門性においても多大な支援をしている。NIPCの活動とは、かなり協調を図っている。総てのセキュリティの管理者は、2週間おきにNIPCの活動の概略を聞くことにしている。また、月一度社内向けに、セキュリティに関するニュースレターを発行している。
- ✓ マーケティングと認識を高めるための活動を支援している。

このような積極的なコメントがある一方で、以下のような消極的なコメントが調査時点での多数を占めている。

- ✓ 支援は行っていない。それを行うだけの時間もないし、得られる便益がわからない。地元の FBI オフィスは、PDD63 に対してあまり積極的に行動していない。

- ✓ 何もしていない。ただ話し合いをするだけである。
- ✓ 認識が欠如していることは非難すべきことであるが、一般に我々はこの種の情報の共有化の活動には加わらないことにしている。
- ✓ 他のメンバー制組織では得られないようなベネフィットがあり、それが、参加して情報を提供することによって生じる不利益を上回るとは考えられなかったので、支援を行わないという意思決定をした。

協同作業のレベルという点において、8つのセクターのいずれが大きな役割を担うことになるか? 業界によっては、協同作業について受容度の高い業界がある。例えば、電力業界は規制に慣れているため、すでに NERC、NPC や API を正式なコンタクト先として使用している。DOT や FAA は、鉄道や航空輸送に大きな規制を行ってきており、その現状に慣れている。一方、石油会社は、政府の規制が過剰であると思われる場合は、米国外に本社を移動させたことさえある。

セクターによる違いに関して書かれた、政府の見方は示唆に富んでいる。金に関わるセクターが一番関心を持たれる。例えば、人々は水道や電気の多少の損失(これは常に起きていることである)には我慢するが、金融のセクターの混乱によってお金が失われた場合には、非常に大きな反応があるだろう。このことは、金融のセクターだけでなく通信のセクターにもあてはまることである。なぜなら、通信は金融処理データの転送に用いられているからである。

緊急サービスのセクターは、主として政府と関連したセクター(FEMA、各州、地域の政府関係機関)である。これらの組織は、サイバースステムの保護についての関心や歴史的な役割をあまり持っていない。これらのサービスを直接的な攻撃から守ろうとする活動についての報告はあっても2、3件程度である。緊急サービスを保護するために割かれているリソースは、主として自然災害や技術的な障害が発生した場合のための、バックアップや冗長性であり、例えば、災害時にコマンドセンターが接続できるようにするための通信機器のバックアップなどが挙げられる。

3.7.1 セクターごとの反応/対応

(1) 通信

より多くの規制を受けているサービス・プロバイダーとベンダーとでは、回答において著しい差異が見られた。サービス・プロバイダーは、PDD63 について明らかに肯定的であった。この違いは、サービス・プロバイダーは直接

的にシステムへの脅威（攻撃など）に関係しており、それらに瞬時に対応しなければならないことで、説明することができる。また、法律の執行機関はサービス・プロバイダーとより緊密な接触があり、システムの使用について定期的に調査を受けていることもその理由として挙げられる。

それに対して、ベンダーは先端技術や市場へ投入するためにかかる時間について関心を持っている。ほとんどの場合、彼等は関連の政府機関と共同で作業する時間（あるいはそのようなことをする習慣）がないものである。ベンダーで生じる問題の影響は、ほとんど社内の問題であり、そのような情報を社外と共有しようというインセンティブはほとんどない。ベンダーの役割は、その製品の安全性を確保することであると考えている。

また、本調査では、通信機器ベンダーに対して、PDD63 による製品開発 / 製品計画への影響についても尋ねているが、PDD63 を受けた製品開発の事例は一件も見られなかった。

(2) 金融

米国の金融業界は、他の産業分野と比べより細部にわたる深いレベルで、政府による規制や監査を受けている。我々のインタビュー調査では、金融機関の関心は専ら規制による要請があるかにかかっている。もし、通貨監督局（OCC: Office of the Controller of the Currency）が、セキュリティ問題に対応するための特定の行動を要求しなければ、金融機関にとってそのような行動をとるインセンティブは非常に低い。

一方、規制および事業上の理由から、金融業界はセキュリティに関して前向きに注目をしている。顧客からのオンラインアクセスと、危険にさらされる金額の多さのために、金融機関はセキュリティに関して徹底的に調査することを迫られている。

(3) ガスおよび石油

インタビュー調査によると、この業界は通信機器ベンダーと同様に、本質的に政府からの関与を嫌っている。この業界の企業はある程度 PDD63 の活動に参加しており、一つの企業は InfraGard を強く支援しているものの、実際には（1999 年中は、）Y2K 問題への対応のためにあまりに忙しく、この種の大きな労力を要するもう一つの問題に同時に対応することはできないということであった。情報を公開することにおける FOIA の問題が、相互依存のプログラムに全面的に参加する上での、大きな妨げとなっていると

いう意見が出された。

(4) 電力

電力業界の企業は、Y2K 問題に焦点を当てて取り組んでいたために、PDD63 の活動に対して時間を割いて取り組むことはほとんど行って来なかった。また、この業界は FOIA について非常に高いレベルの心配をしている。

電力会社は、他の業界に比べてセキュリティに関する脅威は少ないと考えている。しかし、彼等はその状態が今後も続くかどうかについては確信を持っていない。これまでそうした被害を受けなかったのは、幸運だっただけだろうと考えている。また、PDD63 に参加するために必要な費用を払いたいと思っていない。

(5) 交通および運輸

政府は公共交通の産業分野を非常に強く規制している。金融機関と同様に、航空会社は PDD63 に対応する責任を政府の機関、すなわち連邦航空局（FAA）に任せているようである。また、運送業界や鉄道においても同様な心理的傾向がある。海運業界については多少の違いがあるかもしれないが、今回のインタビュー調査では範囲外としている。

(6) 水道

PDD63 の与える影響は、水道業界の場合は他の産業セクターより小さいが、業界としてはこの活動を支援している。インタビューの中で、水道会社は自らの電力、通信、その他の産業界との依存性の認識について、及び、他の産業界の水道に対する依存性の認識について説明してくれた。

水道の供給は、汚染物質の混入による攻撃を受け易いが、技術的な攻撃については次の 2 つの特徴のため受けにくいように見られる。第一には、米国は約 70,000 社という非常に多くの水道会社があることである。そのため、1 社に対する攻撃は、国中への広がりを持ちにくい。第二の特徴としては、この産業で使用されている技術が古いものであるため、攻撃を受けにくいということが挙げられる。

(7) 緊急サービス

緊急サービスに関する政府の視点から見た 2 つの大きな関心事は、資金の問題と FOIA である。資金の問題は、あまり良く計画されていないという認識がある。あるインタビューでは、民間企業が自らの作業やコンプライアンスのための費用を負担し、政府は政府自身のコンプライアンス

や個別の企業を超えて公の利益になることについてのみ費用を負担すべきであるという考えが示された。

(8) 政府サービス

我々は、特定の産業セクターに属さない2つの政府機関からインタビューの回答を得た。これらの機関は、PDD63プログラムを運営する、法律の執行機関および諜報機関に属するもので、正式な形でのインタビューは許されていないが、我々の質問のほとんどについて答えることに消極的であるという状況であったが、どのような懸念を抱いているかについては話をした。その中には、彼等の機関の基本的な性質（情報を公開しない）や米国外の機関に情報が提供されることに対する躊躇が含まれていた。

ある政府のサービス機関は、PDD63の支援についてより肯定的であり、セキュリティの問題に対する注目がより高まるように促進活動をしてきたとのことであった。これらの政府機関は、政府および民間企業の双方について、いかにすればプロジェクトの資金が提供されるか、懸念を強く持っていた。

3.8 サイバーテロの実例

インタビューでは、総ての企業がサイバーテロに遭遇した経験について、情報を提供しようとはしなかった。そのような損失に関する情報の共有は、高いレベルでの相互信頼関係が無い限り、米国では通常は行われぬ。事件が一般に知られた場合でも、そのような情報交換は、インフォーマル・ベースでしか行わない風土がある。典型的には、知人や専門家の同僚の間のネットワークで情報交換が行われるが、それ以外に一般に情報が広がることはない。しかしながら、GTEのように、インターネット上に事件・事故の情報を公開している企業もある。

インタビューの中で述べられた、一般的なサイバーテロの例としては、米国がコソボの中国大使館に対して行った誤爆に対する反応をあげることができる。米国は、世界中から非常に多数の電子メールによる攻撃を受けた。これらの電子メールの発信元はテロリストではないかもしれないが、その結果は、

- 電子メールのオーバーフローによるシステムの性能悪化
- 米国に対する世界の非常に否定的な見方の増大

この事例は、大規模かつ長期のインフラの破壊というよりむしろ、不都合やコストが発生した事例だが、それでもなお実際に起きた脅威である。他にもいくつかの事例があ

り、インフラの崩壊は起きていないが、テロが発生した場合何が起こるかを示唆している。

インフラの制御に関する潜在的な問題の例は、昨年夏のワシントン州 Bellingham のパイプラインの爆発に見ることができる。その事故によって死者が出ただけでなく、Puget Sound 地域のガスの提供が7日から10日にかけて影響を受けることとなった。その破裂がもう少し近隣の都市シアトル側で起きていたならば、燃料の不足は深刻なものとなり、経済的にも影響が発生したであろう。以下が問題の原因であったと思われる。

- 緊急事態や事故への対応プロセスがなかったこと
- 警報システムについて、オペレータに対する適切な訓練が行われていなかったこと
- 同じ日に Puget Sound 地域で発生したメリッサ・ウィルスによる攻撃との潜在的な関係
- 規格品で信頼性の低いオペレーティング・システムを使い制御システムにパッケージソフトウェアを使用しようとする業界の傾向

3.9 企業内でのPDD63に関する教育

インタビューでは教育に関しては直接的な回答はなかった。意義のある教育が行われるためには現在のプロセスの中では、時期が早すぎるというのが我々の認識である。特に重要なリソースを割くということになるのであれば、なおさらである。PDD63の活動はすでに戦略構築のレベルから先へ進んでいるため、我々はこの分野は企業が進んで資金を出し支援する分野になるであろうと見ている。社内での教育に関しては、特に脅威の認識という点での議論はあまりない。

インフラ保護において最も問題となるのは、インフラを所有している会社についての法的責任に関して、法律や政策の明確性がないことである。現在、インフラ提供企業が顧客に対して適切なサービスの信頼性を提供できない場合、その企業が法的責任を負うのかは明確では無い。このことは、物理的設計や制御システム的设计における基本的なセキュリティの欠如のためにインフラへの攻撃が可能となったために、そのようなサービス停止が発生した場合に問題となる。もし、インフラを所有する企業が物理システム、そして、制御システムについて責任を負うのであれば、また、連邦法が彼等にそのような責任があると変更されるなら、企業の教育への投資は急激に増加するであろう。

4. まとめ

以下に本プロジェクトの主要な成果及び結論と考えられる事項を列挙する。

- PDD63 の発令によって、重要インフラの構成要素（ないしセクター）間の相互依存性に関して、問題意識が持たれ、議論の機会が増加した。この相互依存性への関心が、PDD63 の最大の成果であると言える。
- PDD63 は重要インフラへの脅威に対する一般の人々の問題意識のレベルを向上させた。この問題意識の高まりによって、セキュリティ対策にかかる資金や資源が増加するものとみられる。
- PDD63 そのものは、特に新しい技術、製品、セキュリティの制御方式を生み出してはいない。もともと先進的なセキュリティのプログラムを保有し高いレベルのセキュリティへの意識を持っている企業は、特に新しいことやこれまでと異なることに取り組んではいない。
- 多くの企業が、スタッフを会議に派遣することでPDD63 の活動を支援している。また問題認識を高めるためのプログラムをより頻繁に行っているところもある。しかし、PDD63 の直接的な結果として、積極的にセキュリティを改善したり、資源の提供を約束している企業はまだ調査時点ではほとんどないのが実情である。
- PDD63 に関して最も大きな問題は、民間企業と連邦政府との情報の共有である。特に、サイバーテロに遇った経験やその企業の脆弱性に関する情報の共有についてである。政府と産業界とは分断されており、一般的に情報の共有化は行われていない。さらに、企業にとっては米国の情報自由法（FOIA）のもとで、機密情報が公開される恐れがある。
- 同様に、政府機関においても、問題点や脆弱性、米国外での過去の攻撃の事例などを共有化することに対して、極めて神経質な機関が存在している。
- PDD63 のアクションアイテムに対して財源が確保されることは、PDD63 が成功するために重要であるが、これは解決可能な課題とみなすことができる。インタビュー対象のほとんどが、重要インフラのセキュリティ保護を組織化することや、セキュリティ手段を充実するための研究に、連邦政府が資源の割り当てを行うことを期待している。

参考文献

- 1) US Government White Paper, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998
- 2) The White House, *National Plan for Information Systems Protection Version 1.0: An Invitation to a Dialogue*, January 7, 2000