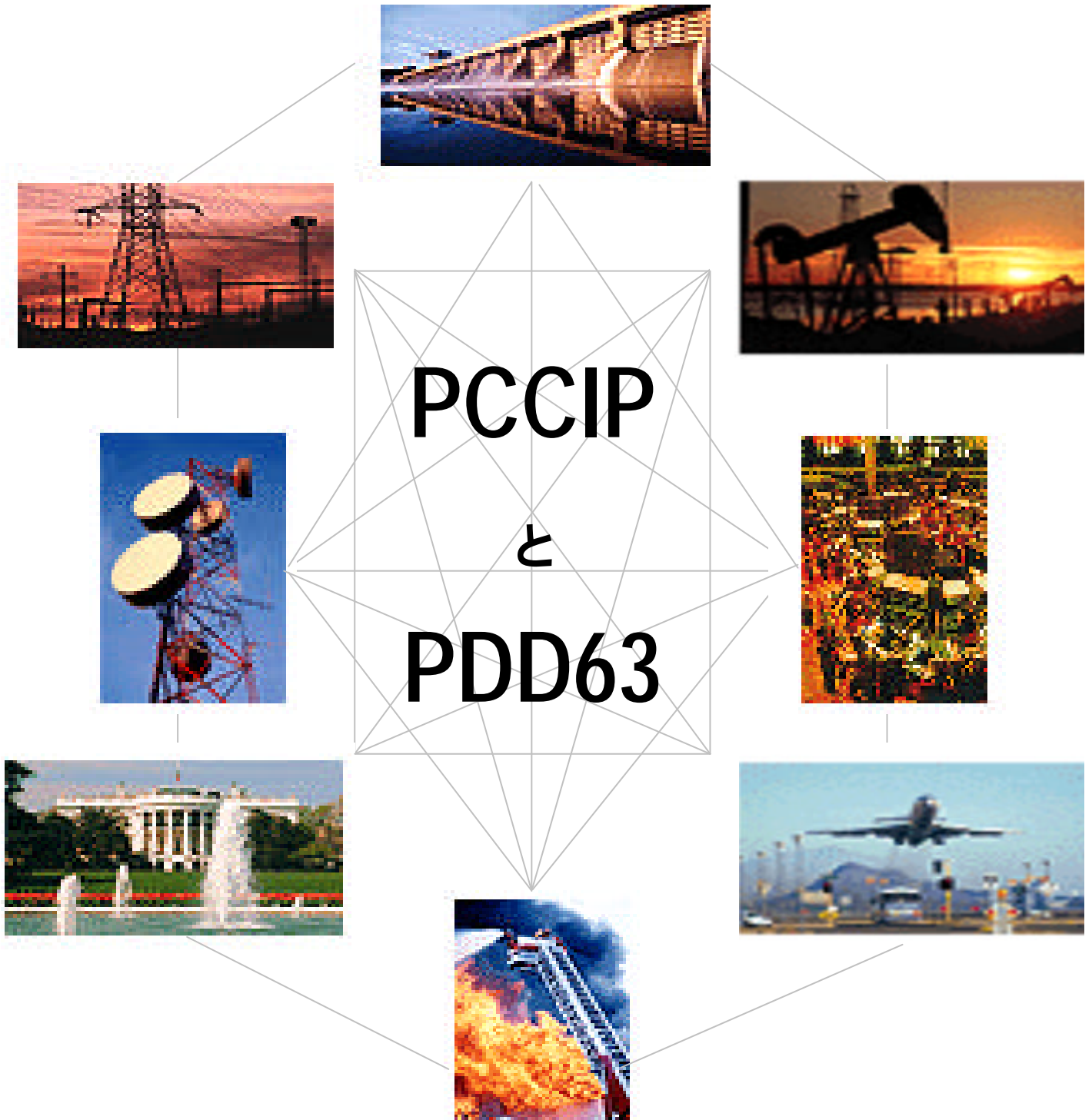


**「重要インフラにおけるセキュリティ対策の事例調査」
調査報告書**

平成12年1月

情報処理振興事業協会



“ 「現代人の悲劇 -

公益にかかる費用を負担することに誰も
関心を抱かないにもかかわらず、費用が
負担されなければ誰もが苦しむような状
況」。¹

¹ Capturing the Importance of Critical Infrastructure Protection

National Communications System Telecommunications Speech Service, VOL. I, Number 3/17/1998

http://www.ncs.gov/N5_HP/Customer_Affairs/Speech_Service/SS98-001.htm

A. はじめに

B. PCCIP とは

C. PDD63 とは

PDD63 に対する産業界の初期反応

PDD63 に対する政府の反応

連邦機関

1. NIPC
2. CIAO

DOD の反応

D. 国の重要なインフラストラクチャ

E. 重要なインフラストラクチャの特性

F. 相互依存の増加

G. インフラストラクチャへの脅威

H. 8 つの重要なインフラストラクチャ

電力産業

ガス / 石油の製造、貯蔵、および輸送

金融と銀行業務

情報と遠隔通信

- a) Financial Services Roundtable
- b) BITS LAB
- c) ISAC

輸送

給水システム

救急サービス

政府の継続サービス

付録

公文書

EO 13010

PDD62

PDD63

重要財団

政府サイトと関連サイトの URL

略語

総括

米国がテロ行為の脅威にさらされていることを米国政府が認識し始めたのは、1960年代の終わりである。オクラホマ州にある Alfred P. Murrah 連邦ビルの爆破とワールド・トレード・センターの爆破という 2 つの出来事は、テロの攻撃に対して米国がいかに脆弱であるか如実に示すことになった。この出来事を機会に、脆弱と見られる米国の他の分野の調査が開始された。

大統領命令 13010(1995 年 7 月) によって設置されたのが、PCCIP(重要インフラに関する大統領委員会)である。PCCIP は、政府と産業界の相互依存性を反映するため、官民の両部門からの人材で構成されている。PCCIP は、米国のインフラストラクチャに対して重要な意味を持つ 8 つの分野を識別している。

電力
ガス / 石油生産
銀行業務と金融

遠隔通信
輸送
給水システム
救急サービス
政府の継続サービス

上記の分野や情報インフラストラクチャは、米国の安全保障や福利にとって重要な意味を持つ。これらの分野はいずれも相互に依存するばかりでなく、遠隔通信やコンピュータに大きく依存するため、サイバー・アタックに対して特に脆弱になる。これらの産業やサービスの大半は民間部門にあるため、重要なインフラストラクチャを保護するための実用的なメカニズムを開発する上で、官民の協力関係を生み出す作業をはるかに複雑なものにしている。

PCCIP は、以下を勧告している。

- 5 年以内に国を挙げて保護に取り組む
- 国の企画局の 1 つとして、Infrastructure Assurance office を設置する
- FBI に本部を置き政府省庁のスタッフで維持される National Infrastructure Protection Center を設置する
- 民間部門によって設立、運営される情報共有分析センターを設置する
- 研究開発に対する資金を増やす
- 国民に PCCIP の調査結果や PCCIP の重要性を伝えるための教育プログラムを開発する

PCCIP による勧告を実現するために、今日に至るまでに、いくつかの政府機関が設置されている。これらの機関には、National Infrastructure Protection Center (NIPC) や Critical Infrastructure Awareness Office (CIAO)が含まれる。各政府機関は、それぞれが支援し、管理する重要なインフラストラクチャと各機関との間の調停役となる高官を任命している。情報共有分析センター(ISAC)では、関連する民間部門に対して、すでに作業を開始している。Financial Services/ISAC は、1999 年 10 月 1 日からサービスを行っている。クリントン政権は、米国のインフラストラクチャ保護に関して、2000 会計年度の予算案で 14 億 6,400 万ドルを要求している。

はじめに

ニュージーランド最大の都市オークランドは 1998 年 1 月 9 日、電力を市に供給している主要高圧電線の 1 つを失った。2 月 9 日に 2 つ目の送電線が失われたことで、混乱はさらに深まった。2 月 19 日には 3 番目の送電線が停止し、2 月 20 日の金曜日午後 5 時 33 分には、最後の送電線が失われた。100 万の人口を持つオークランドは、以後 6 週間で暗黒のなかで過ごした世界初の都市となったのである。

世界の主要都市が、平和時に 6 週間に渡って商業地区に電力をまったく供給できなかったという事態は、想像不可能に思われるかもしれない。ただ 1 つの原因が、この事態を生み出したのではない。都市の電力を停止させたのは、複数のファクターの組み合わせであった。決定的だったのは、非常事態に対する計画が欠如していたことである。この事態は、あらゆる規模の企業に大きな損害をもたらした。電力がなければ、照明、コンピュータ、水から交通信号にいたるまで、すべてが使用できなくなる。ビジネスを通常通りに維持することは、もはや不可能に近い。生活手段をコンピュータに依存していなかったとしても、大半のビルでは窓が開くようには設計されておらず、うだるような暑さが生じた。トイレの設備もすべて機能しなくなった。市民の生活は、極めて困難になった。マンションの 14 階や 20 階で生活することを想像すればよい。エレベーターは動かず、照明は消えたまま、空調は働かず、飲み水やトイレの水洗にも事欠く状態になったのである。ストーブや電子レンジばかりでなく、病院の設備も停止した。電気がなければガス・ポンプも動かないため、ガスを利用することも不可能になった。都市は、文字通りその機能を停止した。電力システムの崩壊を防いだり、崩壊した場合の対処法やメカニズムはまったく準備されていなかったのである。

このケースでは、危機は悪意のある攻撃によってもたらされたものではない。しかし、重要なインフラストラクチャが失われると、その効果がどれほど致命的かを如実に示すことになった。PCCIP が設立されたのは、まさにこの種の事態を取り扱うためである。

EO13010 と PDD63 は、すでに識別した重要なインフラストラクチャに関する問題点を扱うため、各種組織の設立を開始している。本書では、以下について説明している。

- 米国の重要なインフラストラクチャの保護に関連する様々な問題を取り扱うため、公共と民間の両部門によってとられた実際的手段と計画された手段について詳しく説明する。

PCCIP と PDD #63 に対する米国政府の対応

- Financial Services Testing Lab の設置
- Financial Services 情報共有分析センターの設置
- ISAC の設置に向けてエネルギー業界が行っている作業
- ISAC の設置に向けて運輸業界が行っている作業

インフラストラクチャ保護(IP)とその起源

EO 13010

ビル・クリントン大統領が大統領命令(EO) 13010 に署名したのは、1996年7月15日のことである。この法案によって、PCCIP(重要インフラに関する大統領委員会)、Advisory Committee、およびインフラ防衛対策委員会(IPTF)が設立された。



この大統領命令は、米国の主なサービスに対する物理的な脅威(自然的なものや意図的なもの)と「サイバー・アタック」の両方に対処するための計画の必要性を認めている。ワールド・トレード・センターやオクラホマ・シティーで発生した爆破テロ、サリン・ガスによる東京地下鉄への攻撃、ニュージーランドのオークランドで発生した停電などは、公衆のサービスに致命的な崩壊を引き起こしかねない事件や事故を際立たせる結果となった。一方、1980年に発生した Arpanet の崩壊や Melissa ウイルスは、サイバー・アタックの例である。PDD63 が対処しようとしているのは、この種の危機である。

「全国的なインフラストラクチャの一部は不可欠のものであり、その機能の停止や崩壊は米国の防衛や経済の安全保障に重大な衝撃を与えかねない。重要なインフラストラクチャには、遠隔通信、電力、ガスや石油の貯蔵ならびに運送、銀行業務や金融、運輸、水道、救急サービス(医療、警察、消防、救助などを含む)、政府の継続サービスなどが含まれる。これらの重要なインフラストラクチャに対するアタックは、土地建物に対する物理的なアタック(「物理的なアタック」と、重要なインフラストラクチャを制御する情報や通信に対して電子機器、電波、コンピュータなどを使用してもたらされるアタック(「サイバー・アタック」)の2つに分類される。重要なインフラストラクチャの多くは民間部門によって所有され、運営されているため、政府と民間部門が協力し、インフラストラクチャの保護と運営の持続を確保するための戦略を開発することが必要である。」²

². President Clinton, "Executive Order 13010". White House
Washington D.C. United States. July 15, 1996

米国におけるガスと石油パイプライン、送電線、給水設備、公共輸送機関、遠隔通信ネットワークなどはいずれも、物理的アタックばかりでなくサイバー・アタックに対しても脆弱である。米国社会では、公共の電話回線を介するコンピュータ分散処理の活用が急速な伸びを示している。また、これらの先端技術がもたらすメリットの利用に熱心な米国の各種産業は、相互依存の度合いをますます深めている。この傾向は、米国が現時点で享受している経済的な繁栄をさらに活気づけるのに一役買っている。しかし、生産性を向上させ、各種の製品やサービスへのアクセスを容易にしたシステムはまた、米国をアタックに対して脆弱な国家へと変貌させつつある。

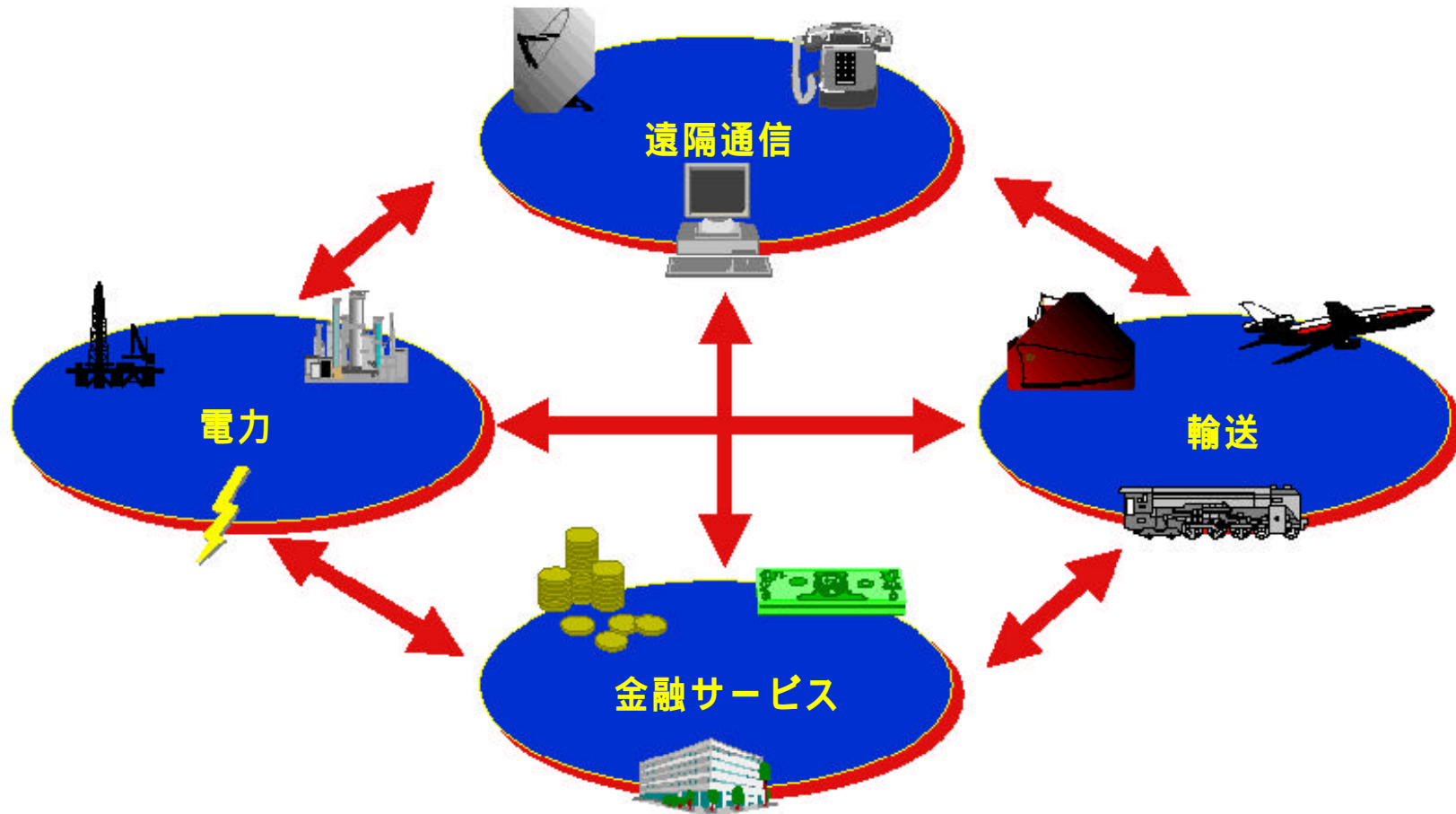
企業が中央処理システムにもっぱら依存し、実際のシステムへのアクセス所有者が比較的少数の人間に限られていたのは昔のことである。いまでは、米国のシステムの大半が分散システムとなり、多くのユーザによるアクセスが可能になった。1950年代には、「発電所や電話交換機が人間をコントローラとして使用した。爆撃機は人間を飛行士として使用し、銀行は Brink ドライバを資金譲渡代理人として使用した。」³ 60年代や70年代になると、大規模なメイン・フレームがビジネスにとって不可欠なものになったが、それらは基本的にはスタンドアロンのシステムであった。1980年代に入ると、パーソナル・コンピュータやインターネットによる分散システムの利用が米国の産業やサービス全般に浸透し始めた。銅製のケーブルを使用していた時代なら、数万の会話を伝送するのに数千本のケーブルを必要とした。いまでは、1本の光ケーブルがそれを可能にしている。

技術の進歩は、効率の改善、生産性の向上、より優れたサービス、低いコストなどを実現する。米国では、あらゆるシステムの効率が改善された。「進歩はインフラストラクチャの効率を向上させたが、結果として余剰が削減され、米国のインフラストラクチャがテロリストの格好の標的になるような状況を生み出した。」⁴ 巧妙に行われるアタックであれば、それが小規模であっても、サービスに致命的な破壊を与えることが可能になった。バックホーでも、使い方によっては同じ結果をもたらすことが可能になったのである。

³ Harry Levins; *Infrastructure Panel taking 'Cyberthreats Seriously'*; St. Louis Post-Dispatch, 06-19-1977, pp03A. 1997

⁴ id

重要なインフラストラクチャ における相互依存



PCCIP とは



PCCIP

PCCIP(重要インフラに関する大統領委員会)とインフラ防衛対策委員会(IPTF)は、大統領命令 13010 によって設立された。PCCIP は 1 年間で費やし、インフラストラクチャに対するサイバー・アタックに対処するための手段を開発した。以下に、それらを具体的に示す。

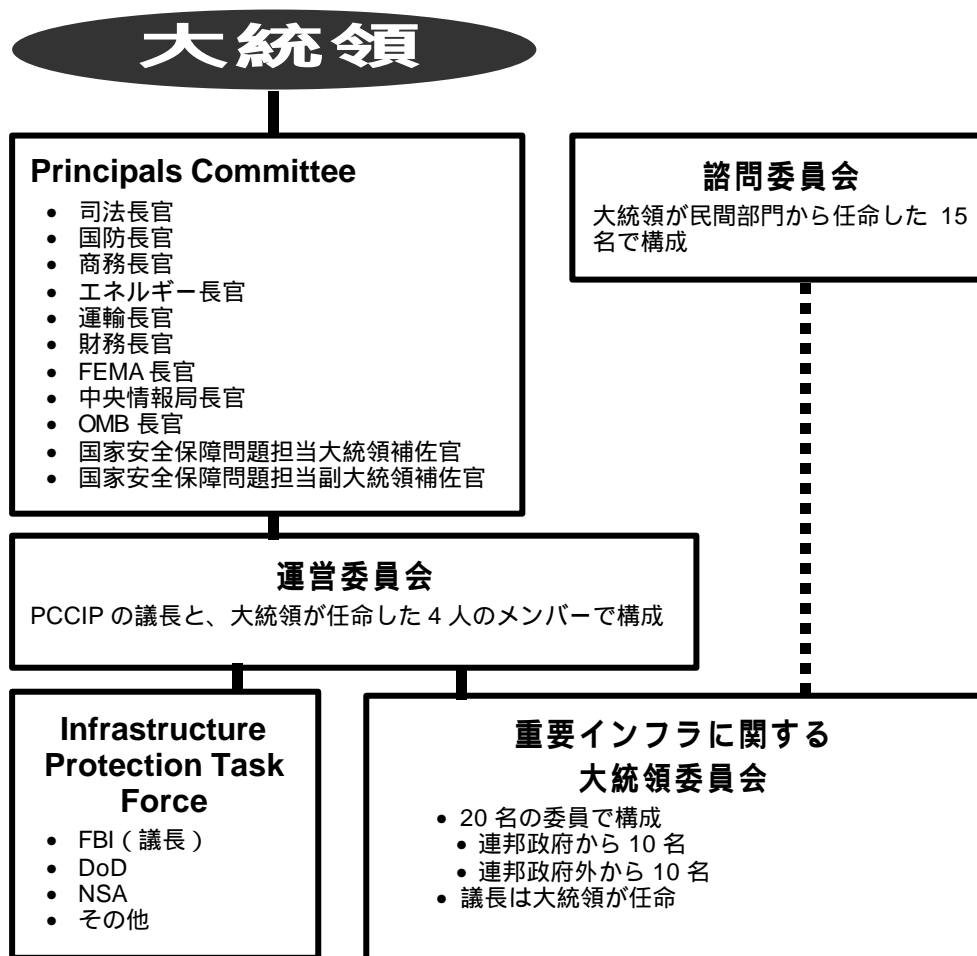
- 以下を識別し、それらと協議する。(i)インフラストラクチャの保全を実行し、支援し、貢献する公共部門と民間部門の構成分子。(ii)重要なインフラストラクチャの所有者と運営者。(iii)公共部門と民間部門に属する他の構成分子で、重要なインフラストラクチャの保全問題に関心があり、しかもそれらの問題に対して異なる考えを持つ構成分子(連邦議会を含む)。
- 重要なインフラストラクチャに対し、その脆弱性の範囲と特性、および脅威を評価する。
- 重要なインフラストラクチャを保護するために、どのような法的、政策的な議題を提出するかを決定し、またこれらの議題をどのように取り扱うかを評価する。
- 重要なインフラストラクチャを物理的アタックやサイバー・アタックから保護し、継続的な稼働を保証するため、包括的な国家方針と導入戦略を勧告する。
- 勧告を実現するのに必要であれば、法的な変更を提案する。
- 報告書や勧告を作成し、準備ができた段階で運営委員会に提出する。⁵

PCCIP が直面する課題は、重要なインフラストラクチャの大半が民間部門によって所有、運営されていることで、複雑なものとなった。この委員会では、政府と民間部門の協力が必要不可欠であった。この協力関係こそが、国家がインフラストラクチャへのあらゆる攻撃に対処することを可能にする戦略を設定するのに必要になったのである。攻撃には、自然災害や物理的アタックもしくはサイバー・アタックなどの外的なもの、故意の破壊や単純な故障などの内的なものが想定された。

⁵ The White House: Office of the Press Secretary, Executive Order-Critical Infrastructure Protection, July 16, 1996

PCCIP の組織

「PCCIP は、連邦政府の内外、つまり州政府や民間産業から参加した最大 20 名のスタッフで構成される。PCCIP を率いる議長は、大統領が任命する。PCCIP は、民間部分の指導者で構成される諮問委員会の忠告を受け入れる。PCCIP は、PCCIP の活動を監視する運営委員会を介して勧告を長官委員会(Principals Committee)に送る。長官委員会は、大統領に提出する前に、すべての報告書や勧告を再検討する。」⁶



⁶ よくある質問に対する PCCIP の答

<http://www.info-sec.com/pccip/web/faq.html>

PCCIP 諮問委員会のメンバー

Mr. Tom Marsh、議長
Ms. Jamie Gorelick、共同議長
Senator Sam Nunn、共同議長
Ms. Maurice Greenberg
Ms. Margaret Greene
Mr. Erle Nye
Mr. Floyd Emerson Wick
Mr. David Campbell
Mr. Charles Lee
Mr. Elvin Moon
Dr. Jeffrey Jaffe
Mayor Sharon Sayles Belton
Mr. Norman Mineta
Mr. Joseph Holmes
Mr. Robert Baxter
Mr. Mort Topfer
Mr. Jerome Davis

委員会の各メンバーの略歴については、付録を参照されたい。

PCCIP の報告書は、重要なインフラストラクチャを保護するのに必要な手段の範囲を特定し、明確化している。米国社会にとって、技術の進歩は幸福なできごとであると同時に不幸なできごとでもあった。傾向は、サービスのコンピュータ化がますます進むことを示しており、公衆電話網(PTN)に依存するインターネット経由のサービスにおいて、それが特に著しい。このため、重要なインフラストラクチャが相互に依存する度合いがますます深まる結果となっている。攻撃に対する米国の脆弱性は、この傾向によってさらに高まっている。また、重要なインフラストラクチャの大半を民間部門が所有しているという事実は、公共部門と民間部門が協力し、米国の脆弱性を改善するとともに、効果的な防止、対応、緩和、回復などを可能にする方針や戦略の立案を促した。PCCIP が行った勧告は、Presidential Decision Directive (PDD) 62 および 63 に盛り込まれている。

IPTF

インフラ防衛対策委員会(IPTF)は、暫定的な政府省庁間の特別専門委員会である。その目的は、PCCIP がその勧告を準備するまでの間、サイバー・アタックに対処するために連邦内の作業を調整することにあつた。IPTF には、連邦捜査局(FBI)のコンピュータ部門、国防総省(DOD)、国家安全保障局(NSA)からのメンバーが含まれていた。IPTF の主なサービスには、以下が含まれていた。

- 連邦政府の内外に存在する専門知識を識別し、調整を行う。
- アタックを検出し、防止し、あるいは停止させるため、あるいはアタックが実際に発生した場合にサービスを回復させるため、重要なインフラストラクチャに対して専門的な指導規定を提供し、促進し、調整を行う。
- 脅威に関する情報を前もって入手した場合は、警告通知を発する。
- 脆弱性を改善するための方法や、インフラストラクチャへのアタックに対処するための方法について、訓練や教育を提供する。
- 将来的な脅威、目標、アタックの方法などを判断するため、アタック発生後の分析を行う。
- アタックを受けている最中かアタック後に、アタックに関する犯罪捜査を推進するために該当する警察当局と調整を行う。⁷

⁷ id

PCCIP は、8 つに分類された重要なインフラストラクチャのいずれかに含まれる企業や組織に調査票(付録 XX を参照)を送付している。また、公的な出向プログラムの一環として、PCCIP は 1997 年の初めから中頃にかけて、米国の様々な都市で一連の公的な会議を開催している。これらの会議では、米国のインフラストラクチャについて意見や関心事を PCCIP に対して表明する機会が講演者に与えられた。会議が開催されたのは、以下の都市である。

カリフォルニア州ロサンゼルス

ジョージア州アトランタ

テキサス州ヒューストン

マサチューセッツ州ボストン

ミズーリ州セントルイス

PCCIP はまた、各種のインフラストラクチャ、民間部門に属するインフラストラクチャの利用者と提供者、学会、州政府や地方自治体の諸機関などに関係する専門家の組合や商業組合との間で会議を開催している。

PCCIP は、1997 年 10 月に報告書を発行している。報告書は、その調査内容を、含まれる産業に共通の特性を表す 5 つの部門に分類している。調査の対象となったのは、以下の 5 つの部門である。

- 情報と通信
- 銀行業務と金融
- エネルギー(電力、石油、ガスを含む)
- 物理的な流通
- 生活に不可欠のサービス(給水、救急サービス、政府の継続サービスなどを含む)

PCCIP が行ったこと :

- 各部門の調査
- 国家にとって重要なインフラストラクチャそれぞれの特性の定義
- 脆弱性の判定
- 各部門を物理的アタック、自然による災害、あるいはサイバー・アタックから保護するための勧告

調査結果

調査の結果、対策が必要と思われる基本的な問題がいくつか判明した。

- 米国の重要なインフラストラクチャ間で相互依存がますます深まっている

- ますます脆弱になっている
- 広範囲にわたる脅威が存在する
- 認識が不足するとともに、国家的な戦略が欠如している

いま、米国は電気エネルギー、通信、およびコンピュータ間の相互関係に多くを依存している。この依存は、爆弾、バックホー、システムの故障などの従来型の物理的な崩壊に対して米国を脆弱にしているばかりでなく、より短時間に行われるサイバー・アタックに対しても脆弱にしている。パーソナル・コンピュータ、電話接続、ハッカーのノウハウを掲載したサイトの出現などにより、テロリストが容易にサイバー依存の米国インフラストラクチャを破壊することが可能になった。また、システムへのわずかな妨害や定期的な妨害が、地域全体に及び停電をもたらすこともある。これは、システム自体が複雑になり、しかもオートメーションの発達で妨害の効果が連鎖的に広がるためである。

これらのインフラストラクチャに悪影響を及ぼす事例も、その種類が多様化している。自然災害や事故の場合もある。火災、洪水、バックホー、地震などの自然現象がサービスを中断させることもある。また、不手際、誤り、怠惰などがシステム中断の原因となることも多い。これらは意図的なものではないが、重大な影響をもたらす可能性があることは否定できない。内部の人間が不公平や不当に扱われていると感じた場合も、大きな混乱を引き起こすことがある。承認されたユーザであっても、システムを混乱に陥れることがある。悪意のないハッカーが国家のシステムやサービスに害を与えたり混乱させることはないとしても、彼らが完成させたツールやテクニックはネットを介して広がり、悪意を持つものなら誰でもその強力で破壊的なテクニックを利用することが可能になる。犯罪者は、銀行強盗などを実行するより、インターネットや PC を使用する方がはるかに見返りが多く、しかも露出が少ないため検挙される可能性が小さいことに気づき始めている。組織犯罪も、マネー・ロンダリングなどの不正行為や、サービスに対する窃盗を隠す方法を見つけだしている。産業スパイも増加している。競合する企業どうしが、知的所有権を相手から盗むことも簡単に行えるようになった。国家も、従来 of スパイ行為に加え、新しい技術がもたらす利点を利用したスパイ活動を行うようになっている。軍部も、未来の戦争が「情報戦」になることを確信している。将来、送電線網や電話網などの国家的なインフラストラクチャに対して、物理アタックとともにサイバー・アタックが使用される可能性がある。

米国のインフラストラクチャがどれほど脆弱であるかを国民の大半が気付いていないのと同じように、政府や民間産業の意志決定者の多くも、システムがいかに簡単に急停止状態に追い込まれるかを十分には理解していない。Y2K問題を考えてみるとよい。いまなを、Y2Kがそれほど大きな問題ではないと信じている人々が存在している。Y2Kは陰謀だと考えている人さえいるのだ。

これまで、インフラストラクチャの保護に対して中央政府が注目したり方向性を示したことはなかった。PCCIPの勧告以前は、政府や官公庁は、米国の重要なインフラストラクチャを構成する製品やサービスの提供者に、製品やサービスの保護と安定した供給を依存していたのである。一部の産業が洗練された保護手段を所有していることは事実であるが、それ以外の産業はまだ出発点に立ったばかりである。

結論

調査は、結論として以下を挙げている。

- 新しい思考が求められている
- 未来を保護するためには、いま行動しなければならない
- インフラストラクチャに対する責任は共有しなければならない

新しい技術がもたらした脆弱性の増大は、検出、保護、問題解決に全く新しいアプローチを要求している。例えば、問題が大きくなる前に、その徴候を検出するための新しいツールの開発が必要になる。また、インフラストラクチャの保護用に開発されたシステムの改善や拡張も必要になる。新しい環境においては、責任の境界が曖昧になる。問題の原因を検出することが困難になるばかりでなく、調査の責任が誰にあるのか、また事件がもたらした損害に対する法的な責任が誰にあるのかを特定することも困難になる。

米国が差し迫った攻撃の危機にさらされているように見えないのは事実である。これまでのところ、米国のインフラストラクチャのいずれかに対し、周到かつ一斉的な攻撃を仕掛けようとした例は皆無である。これが、安全保障について誤った考えを生み出す結果となっている。未知の災害を防止するために、なぜ高価な投資を行わなければならないのだろうか。ハリケーン Floyd によって避難を余儀なくされたカロライナ州沿岸の住民は、集団避難用の案を誰かが作成していたらと願ったことだろう。案が存在すれば、集団避難によって引き起こされたひどい交通渋滞に巻き込まれることもなかったに違いない。また、ニュージーランドのオークランドのビジネス街にある企業が、かくも長時間にわたり電気なしで放置されることもなかつたろう。保護手段や方法が存在

していたら、チェルノブイリや東海村のウラン処理施設で放射線による被害者の数も減っていたに違いない。大局的な観点から緊急事態に対処するための準備が適切でなかった事例は、数え切れないほど存在している。

インフラストラクチャの保護に対する責任は、もはや政府だけが負いきれるものではない。あらゆるインフラストラクチャが相互依存度を深めているいま、公益を保護するために全部門が協力することが急務となっている。これらのサービスの提供者の大半は、民間部門にある。したがって、民間部門は、この分野でより大きな役割を担う必要がある。あらゆるサービスや製造業は、国家の重要なインフラストラクチャの保護に参加しなければならない。その責任は極めて大きいため、1つのサービス実体が他のすべてに対して保護を提供することを期待すべきではない。同時に、1つのサービス実体が他者の行動や責任を指示することも避けなければならない。重要なのは、コンセンサスを得ることである。

PCCIP による勧告

- 広範囲にわたり意識を高め教育するためのプログラムを開発する。
- 産業界の協力と情報の共有を促す。
- インフラストラクチャの保護に関する法律を再検討し、障害となるものがあれば排除する。
- インフラストラクチャの保護に適用可能な技術の発展に役立つ研究開発プログラムを推進する。
- インフラストラクチャを保護するため、重要な決定や勧告を効果的に行うための国家的な取り組みを推進する。

PCCIP は、可能な限り多数の国民の間で、意識を高め教育するための多岐に渡るプログラムの開発を要求している。勧告によれば、教育や意識を高めるためのイニシアチブは、小学校レベルから米国の教育システムに組み込まれ、ハイスクール・レベルに引き継がれるとともに、卒業研究や卒業プログラムには後援が付くようになる。情報技術を学んだ個人に対しては、大きな需要が存在する。また、国民の意識を高めるためのキャンペーンも実施しなければならない。これらの活動によって、米国の各種システムがいかに複雑であるかを国民に認識させる必要がある。

インフラストラクチャの保護をより高いレベルで実現するためには、部門間の協力と、情報を共有するための戦略が不可欠である。事例の情報を共有すれば、傾向を識別できるばかりでなく、問題に対する解決法の開発にも役立つ。「最良の方

法」⁸を使用することが、より迅速に、かつ効率よくインフラストラクチャを保護につながるのである。最良の方法とは、各部門を構成している産業とサービス間の共同作業にほかならない。相互のコンセンサスと分析があれば、情報の損失、サービスの拒否、連鎖反動的な影響などをもたらす可能性がある相互依存関係、物理的アタック、サイバー・アタックを理解するための方法を識別し、開発することが可能になる。これらの方法には、アタックを防止し、損害を軽減し、サービスを回復するばかりでなく、インフラストラクチャを改善するための手段が含まれていなければならない。取り扱う情報が大きくなればなるほど、分析用に情報を官公庁と共有し、インフラストラクチャが意図されたアタックの対象となっているかどうかを評価しなければならない。

産業情報の共有という新しい時代を推進するためには、情報の共有を促進し、強化する法的な改革が必要になる。現存する法律のなかには、企業どうしが情報を共有することを思いとどまらせるものがある。企業が他の企業や政府と情報を共有することが、その企業の不利益となることがないようにするため、新しい保護手段を制定しなければならない。これらの保護手段がなければ、企業は参加することのメリットを見つけないことができず、協力することに否定的になる。

重要なインフラストラクチャを保護するための基本的な技術の一部は、すでに存在している。ただし、それらの技術がより広範囲に使用されることや、技術を改善するための研究開発がさらに必要なことはいうまでもない。また、米国の重要なインフラストラクチャが急速に相互依存の度合いを深めていることによる結果を理解することも必要である。米国の高度に統合されたシステムの力学を研究するため、モデル化ツールやシミュレーション・ツールの開発も必要になる。これらの新しいツールを使用すれば、事件の影響や程度の予測が可能になり、対応策を開発することも可能になる。

PCCIP は、協力関係に対して具体的な勧告を行っている。

- 「各部門のコーディネータは、業界の協力と情報の共有を実現するための中心的な役割を担わなければならない。また、国家的な協力と方針を念頭において部門を代表しなければならない。
- 政府と各部門間のパイプ役となり、また必要に応じて部門のコーディネータを任命するため、連邦政府内に先行機関を設置する。

⁸ PCCIP, “Report Summary Critical Foundations”, October 1997

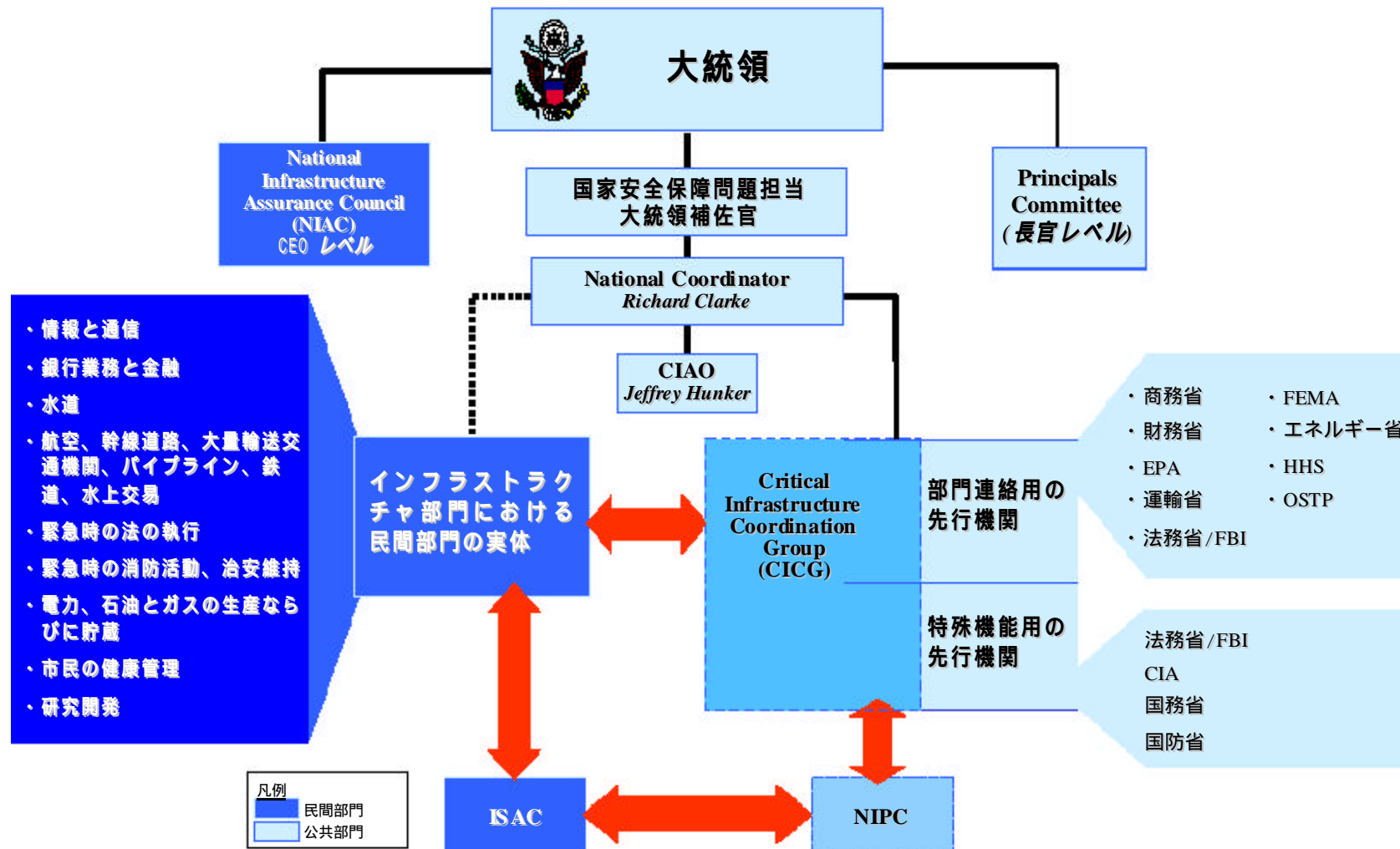
この文書は次のサイトに掲載されている – <http://www.info-war.com/pccip/pccip2/summary.html>

- 業界の CEO、Cabinet Secretaries、州や地方自治体の代表で構成される全米インフラ保障委員会を設置し、方針への助言や運営への参加を行う。
- 情報共有分析センター (Information Sharing and Analysis Centers) を設置し、実際のアタックを偶然に一致する事例から区別しながら、米国のインフラストラクチャに何が発生しているかを現実的に理解するための段階的なプロセスを開始する。
- PCCIP による勧告の継続的な管理や実行に責任を持つスタッフの大半を収容するため、Infrastructure Assurance Support Office を設置する。
- 国家安全保障会議、国家経済会議と密接な関係を持つトップ・レベルの政策制定オフィスとして、Office of National Infrastructure Assurance を設置する。」⁹
- PCCIP の結論は、米国にとってインフラストラクチャの保全を優先事項とすることが絶対に必要であるということであった。技術がもたらす新しい世界では、革新的な保護手段や対抗手段がますます必要になる。この実現に官民の両部門が協力し合っこそ、成功が現実のものになる。」

⁹ PCCIP, “Report Summary Critical Foundations”, October 1997

この文書は次のサイトに掲載されている –

<http://www.info-war.com/pccip/pccip2/summary.html>



PDD62 および PDD63 とは

Presidential Decision Directive 62 - テロリズムとの戦い

この大統領命令は、米国のテロリズム対策を改善することを目的としたものである。その目標は、テロリストによるアタックを抑止し、また防止することにある。アタックが現実に行われた場合は、米国は損害を最小限に食い止め、迅速に対応するため、綿密な調査計画を用意していることが必要になる。

PDD62:

- テロリズムに対処する米国の各機関の任務を強化する。
- 広範囲のプログラムにおいて、各機関の活動を体系化し、明確にする。
 - テロリストの逮捕、告発を行う。
 - 輸送機関の安全保護を強化する。
 - 対策能力を強化する。
 - 米国のインフラストラクチャにとって鍵となるコンピュータ・ベースのシステムを保護する。
- Office of the National Coordinator for Security, Infrastructure Protection, and Counterterrorism を設置する。その対応範囲には、重要なインフラストラクチャばかりでなく、海外でのテロリズムや国内での大量破壊行為が含まれる。¹⁰

Presidential Decision Directive 63 – 重要なインフラストラクチャの保護命令

Presidential Decision Directive 63 (PDD63)は、PCCIP による勧告すべての発動を命じている。

- アタックの警告、抑制、阻止を実現するための案を制定するため、政府は西暦 2003 年までに、アタックに対して脆弱な重要部門やインフラストラクチャそれぞれに対して、関連する民間部門との調整を計るための先行機関を設置する。
- 政府外の各機関それぞれが自らの保護手段を開発する際に、そのモデルとしての役割を果たすことを政府に求める。

¹⁰ The White House , Office of the Press Secretary, Annapolis MD, May 22,1998

Fact Sheet Combating Terrorism: PDD62

Fact Sheet Protecting America's Critical Infrastructures 62

- FBI に全米インフラ防衛センター(NIPC)を設置する。前例を見ない情報共有を実現するため、NIPC には他の政府機関からのメンバーばかりでなく、民間部門からのメンバーを参加させる。
- 政府は、民間部門に情報共有分析センター(ISAC)の設置を奨励する。
- 国の案を策定するため、Critical Infrastructure Assurance Office (CIAO)を設置する。CIAO は、国家的な教育プログラムや意識を高めるためのプログラム、立法、公務の調整も行う。¹¹

米国の重要なインフラストラクチャを保護する PDD63

PCCIP の勧告に基づき、PDD63 は重要なインフラストラクチャを保護するための枠組みを設定している。PDD63 は、西暦 2005 年までに米国が重要なインフラストラクチャのいずれかに悪影響を及ぼしかねない出来事に対処するための準備を整えるため、民間部門と協力して活動する政府機関を設置している。

PDD63 の基盤：

PCCIP は、西暦 2003 年までに信頼性の高い相互接続された強固な情報システム・インフラストラクチャを確立し、また西暦 2000 年までに政府システムの安全保護を大幅に改善することを、その目標に設定している。

- アタックを警告し、また対処するため、国家的なセンターを直ちに設置する。
- 2003 年までに、意図的な破壊行為から重要なインフラストラクチャを保護するための能力を確保する。
- 新たな脅威にさらされる機会を減らすための作業を各部門や局に要求することで、サイバー・アタックや物理アタックに対する連邦政府のインフラストラクチャの脆弱性に取り組む。
- インフラストラクチャの保護を実現するための方法を国内に示すため、モデルとしての役割を果たすよう連邦政府に求める。
- 官民の協力のもとに米国の重要なシステムを保護するという共通の目標を達成するため、民間産業の自主的な参加を求める。
- プライバシーの権利を保護し、自由市場の活用を求める。これは、米国の経済力を抑圧するためではなく、保護することを意図したものである。
- 議会の全般的な参加と協力を求める。

¹¹ The white House , Office of the Press Secretary, Annapolis MD, May 22,1998

Fact Sheet Combating Terrorism: PDD63

Fact Sheet Protecting America's Critical Infrastructures PDD63

また、以下の設置が要求された：

全米インフラ防衛センター(NIPC) - FBI に設置され、FBI、DOD、USSS、エネルギー、運輸、Intelligence Community の各省と民間部門から参加した代表どうしを協力させることをその目的とする。民間部門と協力しながら局間で情報を共有するという前例を見ない試みを行う。NIPC はまた、事件に対する連邦政府の対応を促進、調整し、アタックを抑止し、脅威を調査し、再建作業を監視するための基本的な手段を提供する。



情報共有分析センター(ISAC) - 民間部門による ISAC の設置が奨励されている。



The Critical Infrastructure Assurance Office (CIAO) - 国の案を制定する際に、政府機関や民間部門と共に National Coordinator の活動への支援を行う。CIAO はまた、国の教育プログラムと意識を高めるためのプログラム間や、法と公務間でそれぞれのイニシアチブを調整する。



PDD63 に対する政府の反応

連邦機関

政府は、特定のインフラストラクチャに対して責任を負う政府機関それぞれに、上級連絡担当者をすでに任命している。取り組みの対象となる重要分野は、政府と民間部門のメンバーで構成されたチームが識別する。このチームはまた、防御を改善し、アタックや事故の影響を軽減するための案を制定する。政府はまた、これらの問題を取り扱うため、政府の機関内で率先して作業を進めている。大統領の 2000 会計年度の予算案では、重要なインフラストラクチャの保護のために、28 億 4,900 万ドルが要求されている。2000 会計年度の概算要求で注目に値するのは、以下の点である。

- 新しいワクチンや医薬品の開発費用として、前年度のレベルから 3,000 万ドルを上積み。
- アタックを検出するため、Public Health Surveillance の資金として 1,500 万ドル。
- 新しい都市医療対応チームを設置するための費用として 1,300 万ドル。
- 市民を保護するため、特殊な医薬品を国が継続して購入し、備蓄するための費用として 5,200 万ドル。
- 救急要員を訓練して米国の各都市に配置するための費用、不測の事態で使用される大量破壊兵器に対する対応策や演習用の費用、公衆衛生のインフラストラクチャを強化するための費用として合計 6 億 1,100 万ドル。
- 米国政府の各施設を保護するための費用として 2 億 600 万ドル。
- 病原体のゲノム解読を含む研究開発用として 3 億 8,100 万ドル。
- 核物質に対するワクチン、新型治療、検出と診断、汚染除去、および廃棄。
- 重要なインフラストラクチャとコンピュータの安全保護用に 14 億 6,400 万ドル。大統領が PCCIP を設置して以来、2 年で 40% の増加となる。重要な点を次に示す。
 - Critical Infrastructure Applied Research Initiative (5 億ドル)。
 - Intrusion and Detection Systems : 連邦機関用システムの開発と評価に、200 万ドルが支出される。
 - ISAC の立ち上がりを支援するための費用として 800 万ドル。
 - コンピュータ・ネットワークへのアタックに対処するための Cyber Corps の設置。
 - コンピュータ・サイエンスの学生を再訓練し、維持し、募集するための新しい奨学金制度の研究用に 300 万ドル。¹²

¹² Office of the Press Secretary, “Funding for Domestic Preparedness and Critical Infrastructure Protection”, The White House, January 22, 1999; fact sheet

<http://www.fbi.gov/nipc/fact2/htm>

全米インフラ防衛センター(NIPC)

NIPC は、1998 年 2 月に設置された。NIPC は、官民の両部門における重要なインフラストラクチャの所有者や運営者と、インフラストラクチャに関連する連邦、州、地方自治体の各機関で構成されている。



NIPC の任務は、

「我々の重要なインフラストラクチャを目標とするか、インフラストラクチャが巻き込まれるような侵略や違法行為を、その原因にかかわらず、検出し、抑制し、評価し、警告し、対応し、調査すること」である。¹³

NIPC は、事件にかかわる多数のソースからデータを収集し、分析する。これらの分析を基に、最も影響を受ける相手に情報や警告が伝えられる。NIPC の役割は、重要なインフラストラクチャの防衛(Critical Infrastructure Protection - CIP)の強化にあるのではなく、多数のソースから情報を収集して分析し、関係のある消費者すべてに警告することで、侵略や違法行為の防止を手助けすることにある。事件が発生すれば、NIPC は中心となって危機に対する対応や調査を行う。NIPC は、FBI の一組織ではない。NIPC は、FBI の内部に設置され、政府省庁間の活動を行う。

¹³ National Infrastructure Protection Center, "OutreachInfragard"

<http://www.fbi.gov/nipc/nipc/outreachinfragd.htmact2/htm>

CIAO

Critical Infrastructure Assurance Office (CIAO)の役割は、1998年6月に Jeffrey Hunker が下院を前に発表した声明に最もよく表されている。



「PDD63 が CIAO に課したのは、各部門の案を *National Infrastructure Assurance Plan* に統合すること、米国政府自体が重要なインフラストラクチャに依存している実体の分析を調整することである。CIAO はまた、全国的な教育プログラムと意識を高めるためのプログラムや、関連する立法や公務の調整にも助力をおしまない。簡単に言えば、CIAO は国家的な案を制定する列車を駆動するエンジンの役割を担っている。PCCIP の前委員やスタッフの技術や才能をフルに活用できることは、非常に幸運なことである。我々は、*National Coordinator* を補佐し、国の重要なインフラストラクチャを、意図的で悪影響を及ぼすアタックから保護するための国家的な案の制定に助力できるものと期待している。」¹⁴

資金が投下される研究イニシアチブ：

- 連邦機関の各システムに生じた異常を検出し、システム管理者にアタックを通知できるように設計された人工知能能力。
- 政府機関が使用するソフトウェア・コードに埋め込まれる「トラップ・ドア」など、各種の安全保障を脅かす要因を識別するための自動化技法の設計。

¹⁴ Hunker, Dr. Jeffrey A., “Infrastructure Protection Information Assurance , Congressional Testimony, 06-11-1998

DOD の反応

「かつては、米国のインフラストラクチャを攻撃するには、物理的な距離と物理的な国境を乗り越えなければならなかった。いまでは、敵対者が任意の場所から即座にインフラストラクチャの中心にアクセスし、そのアクセスを利用して危害を加えることが可能になった。」 - Robert T. Marsh, Chairman of the PCCIP



コンピュータ・システムに対する安全保障の要望は、歴史的には国防や諜報にかかわる機関から生じたものである。これらの機関は常に、そのシステムの保護に関心を持ち続けるとともに、研究開発に多大な資金を投資してきた。その事実にもかかわらず、米国のシステムがアタックに対していまなを脆弱ではないかとの懸念がある。国防省に向けられたサイバー・アタックの報告数は、1999年11月までに18,433件に達している。しかも、すべての侵入や事例が報告されているわけではない。このため、関係者は実数がこれよりはるかに多いものと信じている。サイバー・セキュリティやサイバー戦は、成長産業であるとさえ言われ続けている。

米国をサイバー・アタックから防衛し、保護するプロセスを開始するため、すでにいくつかの手順がとられている。1999年9月には、Defense Computer Forensics Labが設置された。その目的は、「軍部が巻き込まれるようなスパイ行為、殺人、その他の犯罪が発生した場合に、電子的な証拠を解明することである。」¹⁵ 軍部は、ペンタゴンにJoint Task Force-Computer Network Defenseをすでに設置している。その目的は、ペンタゴンのコンピュータ、LAN、長距離ネットワークの防御を組織化することにある。このシステムは、1999年10月に公式にペンタゴンの戦闘任務の一部となった。このシステムは24時間中、軍部のコンピュータ・ノードを監視している。¹⁶ また、コンピュータ・ネットワークへの攻撃を防ぐため、1999年10月には独立したサイバー戦センターが設置されている。このセンターは、アタックに対する戦術的な警告を提供するとともに、アタックの評価を行う。また、連邦緊急事態管理局の指示のもとに、インフラストラク

¹⁵ Bridis, Ted, "High-Tech Crime – Fighting Lab Unveiled",

http://www.infowar.com/mil_c41/99/mil_c41_092599a_j.shtml

¹⁶ Brewin, Bob & Harrell, Heather, "U.S. sitting duck, DOD panel predicts," 11/11/96 Information Warfare

チャの機能に対して緊急対応演習を行うことができる。¹⁷ このセンターは、システム、ネットワーク、およびインフラストラクチャの設計を実質的に担当することになる。コンピュータやネットワークの安全保障の分野における研究開発は、軍部の重要な関心事であり続けている。PCCIP や PDD63 が設置される以前は、意図的で悪意のあるアタックから生き残るための対策や、悪意を持ったソフトウェアを検出し、排除するための対策はほとんどとられていなかったのである。

軍部は、サイバー戦が急速に現実のものとなることを固く信じている。米国のインフラストラクチャを攻撃するための戦力はすでに現実のものとなっている。コソボ紛争が発生したとき、政府内の多数の部門や機関が Web サイトの停止に追い込まれた。これは、ハッカーによってサイトが書き換えられたためである。損害は致命的、恒久的なものではなかったが、サイバー・アタックが米国のシステムに及ぼす影響の大きさを示すことになった。米国の軍部は、セルビア空軍の防衛システムを制御するコンピュータを標的とした電波妨害用の航空機を実際に使用している。しかし、これば別の問題を生じることになった。米国の軍部は、戦略的な活動を停止させるため、セルビアの多くの標的に対して総力をあげてサイバー・アタックをしかけることを考えていたが、アタックを実施しないことを選択した。軍の目標を達成するために市民を不必要に苦況に陥れることは、戦争倫理に違反すると感じたのである。アタックを実施していれば、戦争犯罪であると非難される結果になったことだろう。

サイバー防衛やサイバー戦に対する総体的な戦略を考案する際に米国政府が直面したこれらの問題は、数が多いばかりでなく、手強いものである。戦争に対する新種の脅威をかわすため、米国政府は次の数年間にわたり、50 億ドルから 100 億ドルを出費するものと予測されている。¹⁸ DOD は、Joint Vision 2010 において「米国は情報で優位に立たなければならない。つまり、途絶えることなく流れる情報を収集し、処理し、伝達しながら、敵対者による同種の活動は、それを利用するか拒否するための能力を持たなければならない」と声明している。DOD は、これからの軍事力を次のように想定している。

- 現在の兵力と比較して規模は小さくなるが、より優れた装備を持つ。

¹⁷ Becker, Elizabeth, "Pentagon Sets up New Center for Waging Cyberwarfare", The New York Times News Service, 08/10/1999

¹⁸ Munro, Neil, "National Journal", 3/27/99

http://www.infowar.com/mil_c4i/99/mil_c4i_032999c_j.shtml

- すべてのレベルにおいて技術的な優位に立ち、軍が次の活動を行うことが可能になる。
 - より早く危険を察知することが可能になる。
 - 全体的な状況や地域的な状況において、詳細な情報を得ることが可能になる。
 - 戦場との間だけでなく、兵士との間で通信を維持し続けることが可能になる。
 - 迅速な対応(週単位ではなく日単位)を可能にする優れた後方支援能力を持つ。
- 迅速な再配置、補強、再投入が可能になる。
- 正確な標的設定やより長距離の攻撃能力を持つことで、多数の兵員を危険にさらすことなく軍事目標の達成が可能になる。
- 後方支援用に先端技術を駆使した通信システムや情報システムを使用することで、集結時間の短縮が可能になる。

国の重要なインフラストラクチャ

重要なインフラストラクチャの特性

PCCIP は、インフラストラクチャを次のように定義している。

「関連する活動に従事する個々の企業の集団以上のもの。人が作り上げ、それぞれが独立し、しかもその大半が民間によって所有されるシステムやプロセスのネットワークで、お互いに協力し合い、相乗効果をあげながら機能し、必要不可欠な商品やサービスを継続して提供し、配布するものを指す。」¹⁹

これらのインフラストラクチャは非常に重要であるため、その機能が停止したり破壊されると、国家の経済や防衛に致命的な影響を及ぼしかねない。これらのシステムは、物理的なものであるかサイバー・ベースのものであるかに関係なく、米国が最小限の活動を行うために必要不可欠なものである。重要なインフラストラクチャには、遠隔通信、エネルギー、銀行業務と金融、輸送、給水システム、および救急サービスが含まれる。

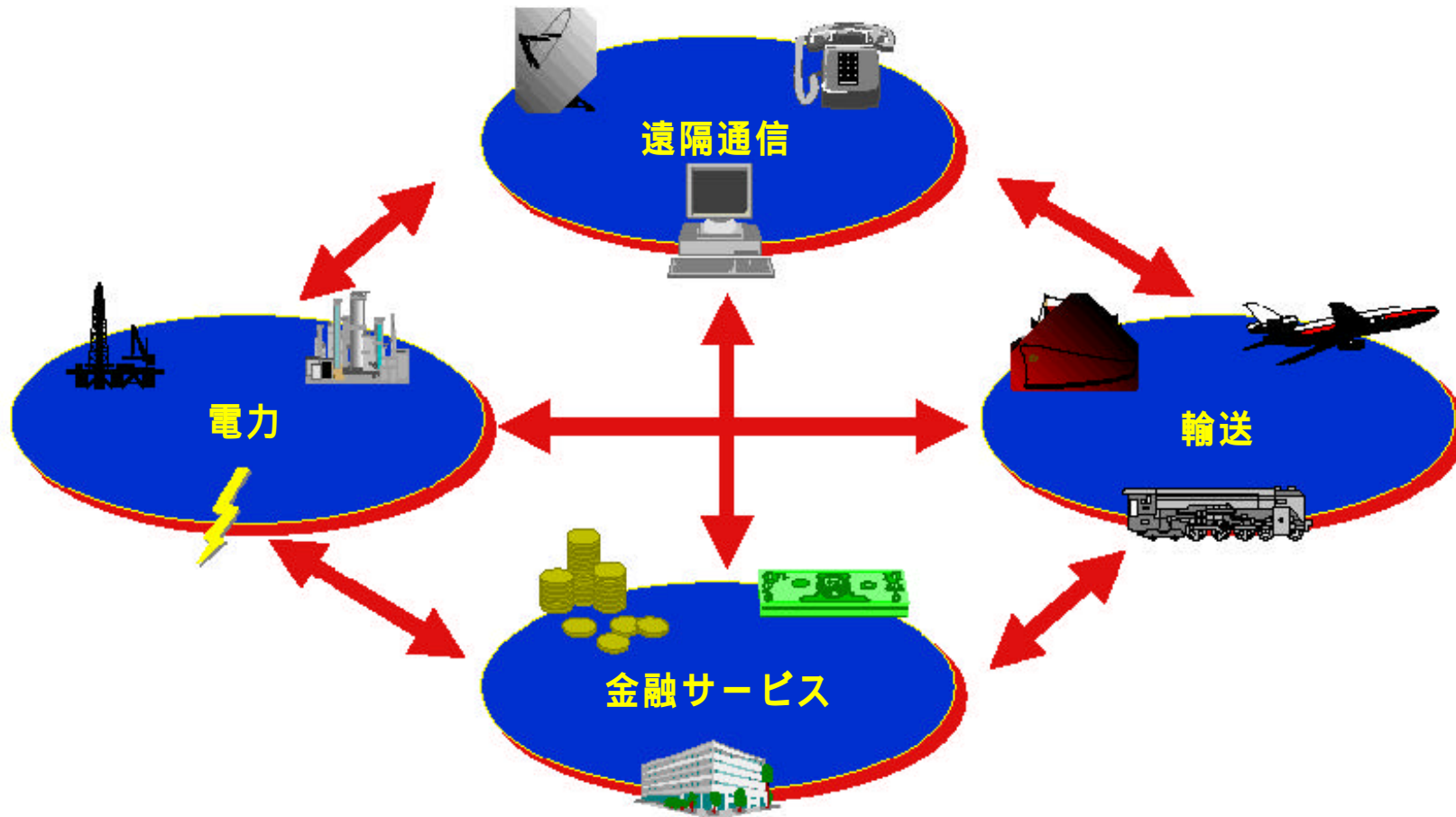
相互依存の増加

歴史的に見ると、これらのインフラストラクチャは物理的、論理的に独立していた。これらのシステムが相互依存することは、ほとんどなかったのである。コンピュータや遠隔通信の新たな進展は、人々が生活する方法、通信する方法、仕事のやり方や場所、商業に携わる方法などを大きく変化させた。洗練された遠隔通信機能や計算機能に対する需要が増加するとともに、情報への需要が増加し、さらに容易にアクセスできることが求められるようになってきている。インターネットの利用も、飛躍的に伸びている。企業は、生産性の向上と原価の切り下げを絶え間なく追求するため、自動化をさらに押し進めている。その結果、インターネットや分散システムを使用してビジネスを行う機会がますます増えている。各部門の企業は、これらの自動化システムを遠隔通信ネットワーク経由で使用し、企業活動の管理や運営を行っている。この結果、米国の重要なインフラストラクチャは、これらのシステムの利用可能性や信頼性に依存するようになっ

¹⁹ PCCIP, “Critical Foundations – Protecting America’s Infrastructures,” Chapter 1, page 3, 10/97
http://www.info-war.com/pccip/pccip2/report_index.html

ている。10 年前は電力だけが最重要の分野であったが、いまでは遠隔通信産業やコンピュータ産業も他のあらゆる部門が活動するうえで不可欠になっている。電力が失われると、遠隔通信の機能が失われる。遠隔通信の機能が失われると、あらゆる部門で生産が停止する結果となる。

重要なインフラストラクチャ における相互依存



インフラストラクチャへの脅威

重要なインフラストラクチャに対する脅威は、様々な形でもたらされる。

- 天災や不慮の事故によるサービスの停止。ハリケーン、洪水、トルネード、地震など。
- 不手際、誤り、怠慢などによってもたらされる不慮の出来事。これには、能力の不足、好奇心、偶発的な行為などによって人が引き起こす事例が含まれる。
- 違法行為や犯罪行為によって引き起こされる事例。ハッカーによる行為、金融やクレジット記録の操作などの犯罪行為、サービスに関する窃盗などが含まれる。
- 組織犯罪によるサービスの悪用。組織犯罪は、これらのサービスを利用して犯罪行為を偽装したり隠蔽することがある。
- 内部の人間による事例。雇用主から正当に扱われていないと感じたとき、恨みから事件を引き起こすことがある。
- 産業スパイ。冷戦が終結するとともに産業スパイが増加している。
- テロ行為。テロリストは、インターネットへの電話接続を経由して多大の損害を引き起こすことが可能なことを理解しつつある。
- 諜報活動。国によっては、他の国家の機密を探り出すのに熱心なことがある。

効率改善への意欲は、余剰をなくすことと同じ意味を持つようになった。そのよい例が、分割前の AT&T である。Ma Bell と呼ばれた同社は、その方針として物理的な多様性を維持していた。つまり、音声やデータの送信を、異なる場所、技術、物理的インフラストラクチャを持つ複数の経路を経由して行うことができたのである。国家的なネットワークを常に利用可能な状態におくため、地下ケーブル、マイクロ波、衛星が併用された。AT&T は、物理的な多様性をとおして、ネットワークの信頼性に対する責任を全うしていた。しかし、規制緩和に伴い、責任の所在は顧客に移動したのである。

国家の 8 つの重要なインフラストラクチャ

PCCIP は、重要なインフラストラクチャとして、次の 8 つを定義している。

遠隔通信

対エンドユーザやエンドユーザ間の電子的な通信の伝送や交換を支援するネットワークやシステム(ネットワーク接続されたコンピュータなど)。

電力供給システム

発電所や送電線網。これらは、エンドユーザが通常の活動を行い、活動を維持できるよう電力を発生し、供給する。また、電力供給システムに必要な不可欠な、燃料の輸送や貯蔵が含まれる。

ガスと石油の製造、貯蔵、および輸送

天然ガス、原油、精製済み石油、および石油を原料とする燃料の貯蔵施設、これらの燃料用の精製処理施設、およびガスや石油に依存するシステムにこれらの生活必需品を輸送するためのパイプライン、船舶、トラック、鉄道など。

銀行業務と金融

あらゆる種類の金融取引にかかわる組織。小口金融や商業銀行業務を行う組織、投資機関、証券取引所、商社や予約システム、および関連して活動する組織、政府組織、および支援組織など。活動内容には、貯金を目的とする保管、収入を目的とする投資、支払を目的とする売買、ローンや他の金融手段をとる支払いなどが含まれる。

輸送

航空、鉄道、幹線道路、船舶、水路、および支援システム。商取引、政府の業務、個人的な用事などを支援し実行するため、人や商品のある場所から目的地まで運ぶ。

給水システム

水源、水源地と貯蔵施設、水路やその他の水輸送システム、濾過洗浄システム、パイプライン、冷却システムや、過程や産業設備に給水する設備すべて。廃水処理用や消化用のシステムも含まれる。

救急サービス

医療、警察、消防、救助などのシステムとその隊員。公衆衛生や安全に関する緊急事件に個人や社会が巻き込まれた場合に呼び出される。

政府の継続サービス

連邦、州、地方自治体の各レベルにおける業務やサービスで、公衆衛生、安全、福利など、国家のシステムが機能するために不可欠なもの。²⁰

これら 8 つのカテゴリは、さらに 5 つの産業部門に絞り込まれている。

- 情報と通信
- 銀行業務と金融
- エネルギー(電力、石油、ガスを含む)
- 物理的な輸送
- 生活必需サービス(給水、救急サービス、政府の継続サービスなどが含まれる)

²⁰President's Commission on Critical Infrastructure Protection, "Our Nation's Critical Infrastructures, Some Working Definitions"

<http://www.infowar.com/>

情報と遠隔通信

一部の統計を見ると、米国が情報と遠隔通信部門をどれほど使用しているか、またどれほど依存しているかをよく理解できる。

- 世界のコンピュータ・パワーの 42%
- 世界のインターネット資産の 60%
- インターネットへの 1 日の接続時間が約 2 億時間
- 大企業の 90%、小企業の 75% が LAN を所有
- 連邦政府が情報技術に対して費やす金額は年間約 400 億ドル
- GDP の 50% が情報関連
- 2002 年までに米国が E コマースに費やすと予測される金額は 3000 億ドル²¹

この部門に含まれるのは、遠隔通信、コンピュータとソフトウェア、インターネット、衛星、および光ファイバーである。遠隔通信は、重要なインフラストラクチャの重要性で 2 位にランクされる。インターネットを介する分散処理は、比較的短期間のうちに現在の社会に不可欠なものとなった。公衆交換回線網(PNS)を經由してインターネットを利用することが可能になり、企業は各種の活動を迅速に、安価に接続できるようになった。

「公衆交換回線網(PNS)は、コンピュータ・システム、人々、組織、機能実体などの間の接続の大半を提供するという点で、国家の関心事のなかでも特異なものである。」²²

PSN の弱点は、多数によってアクセス可能であり、しかもその外部設備があまりに露出されているため、物理的アタックやサイバー・アタックに対して極めて脆弱なことにあ

る。
遠隔通信産業は、自らの保護という点では最も進んでいる部門である。例えば、1963 年 8 月 21 日付けの大統領覚書によって、NCS が設置されている。その目標は、連邦政府用に、信頼性の高い、相互操作が可能な遠隔通信システムを設計することであった。また 1984 年には、National Coordinating Center for Telecommunications (NCC)が設置されて

²¹ Nancy J. Wong, “The Nation’s Central Nervous System”, PCCIP- Information and Communications Sector Presentations, Briefing to the Advisory Committee, September 5, 1997
<http://www.info-war/pccip/>

²² Ware, Willis,H., “The Cyber-Posture of the National Information Infrastructure, October 1997, Rand Publications
<http://www.rand.org/publications/MR/MR976/mr976.html>

いる。NCC は、国家の安全保障と緊急事態を念頭に、その準備の開始、調整、修復、再構築などを補佐する。NCC は、産業界と政府で構成される共同の組織である。

大統領命令 12382 によって設置されたのが、President's National Security Telecommunications Advisory Committee (NSTAC) である。NSTAC の目的は、遠隔通信に関して産業主体の分析と勧告を大統領に提示することである。NSTAC は、30 名に足りないメンバーで構成される。メンバーは、産業界の指導者であり、通常は様々な遠隔通信企業を代表する CEO である。1991 年には、これらのメンバーによって Network Security Information Exchange (NSIE) が設置された。NSIE は、不正侵入問題に関する情報を交換できるサイトを提供する。問題には、公共のネットワーク、ソフトウェア、およびデータベースに影響を及ぼす侵入や不正操作などが含まれる。

PCCIP は、情報通信インフラストラクチャの期待を表すために、「Network Assurance(ネットワーク保証度)」の語を新たに作成している。

「ネットワーク保証度とは、ネットワークの相対的な信頼性、安全保障、伝送クォリティと、顧客によるタイムリーなアクセスを示す用語である。構成要素のレベルでは、ネットワーク保証度は、ハードウェアやソフトウェアの故障、セキュリティに対する侵入、渋滞による過負荷、定期的なダウンタイム、劇的な自然災害、人的な誤りなどによって低下する。サービス・レベルでは、ネットワーク保証度は、ネットワークを構成しているシステムどうしの相互作用によって大幅に損なわれる可能性がある。ネットワーク保証度は、ネットワーク・セグメント(これも PCCIP の造語の 1 つ)に関する問題を抱えている。ネットワーク・セグメントには、インターネット、CATV、無線サービス、衛星主体サービスなどがあり、これまではそれぞれが明確に区別されてきた。しかし、これらのセグメントは集中化が進み、21 世紀の初頭には 1 つのインフラストラクチャに統合される可能性が高い。」²³

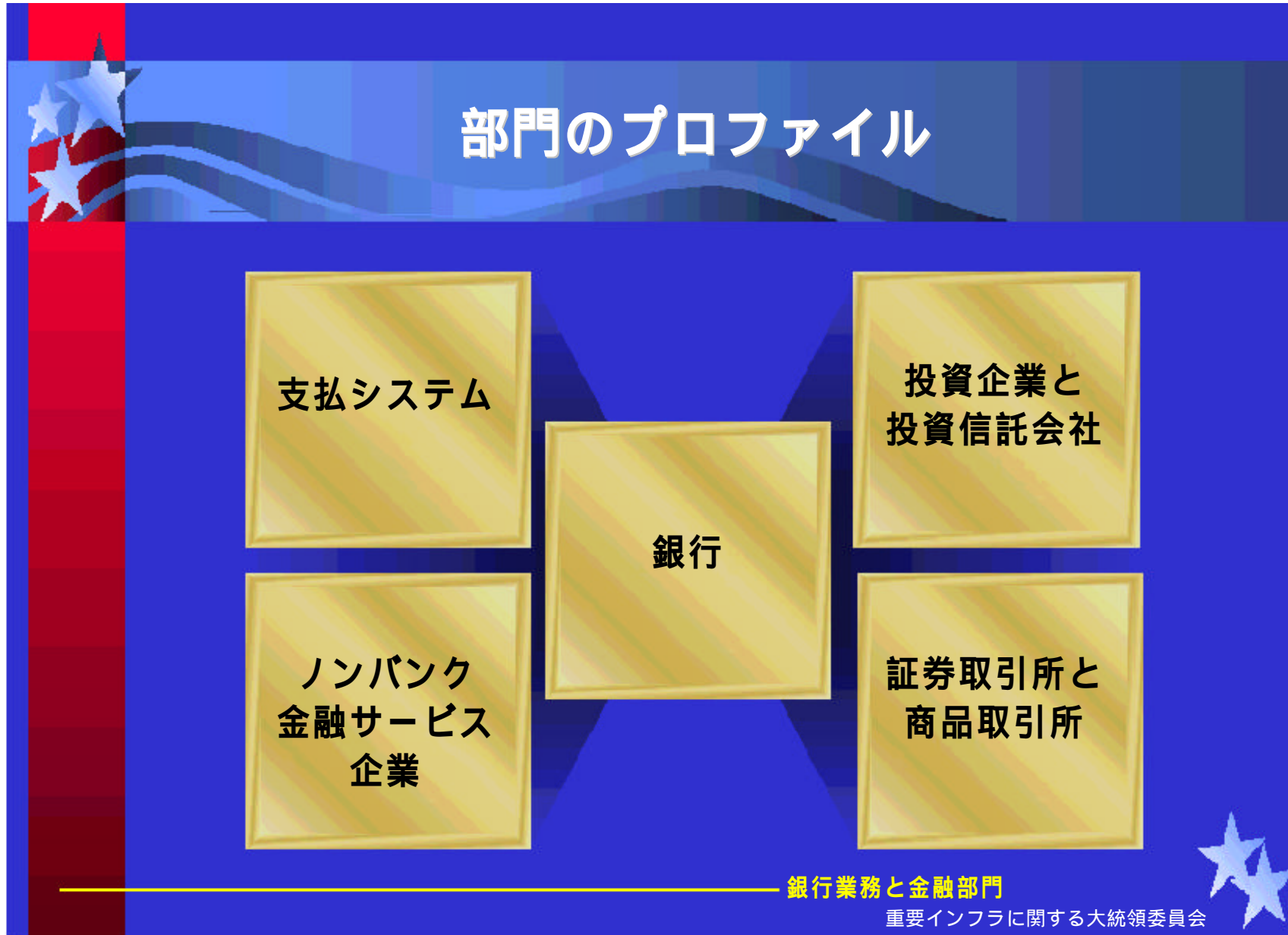
²³ Reagor, Barbara, "A world with New Rules: How to manage risk in the land of Interconnections and Interfaces. Vol. 102, America's Network, 02-15-1998, PP S5 (6).

http://www.elibrary.com/getdoc.cgi...143038@library_j&dtype=0~0&dinst=0

PCCIP と PDD #63 に対する米国政府の対応

1995 年、ホワイト・ハウスは Information Infrastructure Task Force (IITF)を設置している。IITF の目的は、政府や国のニーズに合った包括的な遠隔通信ならびに情報政策を制定することである。IITF は、政府、産業界、労働組合、学会、公益グループ、州政府と地方自治体のメンバーで構成される。

PDD63 が設置されて以来、前述した委員会にはいずれも、PDD63 の重要案件を処理するため、インフラストラクチャの保護(IP)専門の下部組織が追加されている。



銀行業務と金融

銀行業務と金融部門は、あらゆる種類の金融取引にかかわる組織として定義されている。これには、小口金融や商業銀行業務を行う組織、投資機関、証券取引所、商社や予約システム、およびそれらに関連して活動する組織、政府組織、および支援組織などが含まれる。活動内容には、貯金を目的とする保管、収入を目的とする投資、支払を目的とする売買、ローンや他の金融手段をとる支払いなどがすべて含まれる。

米国の金融サービス市場は、世界の市場の 40% を占めている。これは、金額にして約 7 兆ドルに相当する。金融サービス市場は、政府や産業界ばかりでなく、国民にとっても中心的な役割を果たしている。また、コンピュータ、分散処理、インターネットなどを採用することで、製品やサービスの自動化に最も熱心に取り組んできた部門でもある。この部門は、情報通信部門にほぼ完全に依存している。そのビジネスの性格上、この部門はアタックから自らを保護するため、常に最先端の防衛策を採用してきた。しかし、この部門の防衛メカニズムは、いかに印象的であるとしても、直接、間接的なアタックに対しては、いまなお脆弱である。また、PSN(公衆交換回線網)の停止によって致命的な影響を被るのも、この部門である。当初、相互依存がまだよく理解されていなかったため、この部門は PDD63 による勧告を受け入れるのに積極的ではなかった。産業界は、政府の直接的な介入や法的責任を恐れるあまり、事例情報を競合相手や政府と共有することに乗り気ではなかった。この部門が PDD63 に対応するためには、悪い評判によって一般の信頼性が失われることに対する恐れを克服する必要があったのである。

Financial Services Roundtable や President's National Security Telecommunications Advisory Committee (NSTAC) の影響力により、金融部門は指令の勧告を実行するうえで、大きな進歩を遂げている。

Financial Services Roundtable は、銀行業務と金融団体のメンバーで構成される組織である。その任務は、その Web サイトに次のように記されている。

Financial Services Roundtable の意図は、次の 3 つの方法で、最大規模を持つ金融サービス企業の指導力を統一することである。

1. *米国金融サービス業の指導者が、活気に満ち競争力のある市場を形成し、国家経済を成長させるような最重要の公的な利益問題を決定し、また影響力を行使できる第 1 位のフォーラムとすること。*

2. 連邦の立法、規制、および司法の各フォーラムにある会員企業の顧客や株主の利益を促進すること。
3. 競争力があり統合された金融サービスのメリットを、米国の国民や政策立案者に対して効果的に伝えること。

Financial Services Roundtable の会員は、米国において総合的な金融サービスを行っている営利目的の企業に制限される。また、米国の総合的な金融企業の上位 150 社から選ばれた 100 名の会員で構成される。新規会員となる企業からの最初の代表は、その企業の CEO でなければならない。会合や議論を繰り返すことで、金融業界はそのスタンスを変化させてきた。業界自体が何らかの行動を起こさなければ、連邦政府が介入し、新しい法律を制定するとの認識があったためである。米国における最も規制の厳しい業界の 1 つとして、会員はあらゆる犠牲を払ってでもこの動向を回避すべきであると感じていた。また、事例情報を匿名で提出するための方法が考案できれば、Financial Services Information Sharing and Analysis Center (ISAC) の設置が可能であるとの合意に達した。

BITS

Banking Industry Technology Secretariat (BITS) は、Financial Services Roundtable の技術グループである。BITS は、1996 年に設置された。その目的は、開かれた環境のなかで電子銀行業務(エレクトロニック・バンキング)や電子商取引(E コマース)の成長や発展を促進し、また金融組織やその顧客の利益となるよう、金融ソフトウェア、アクセス装置、ネットワーク、および処理機能における選択肢の増加や効率の改善を促すことにある。BITS は、金融サービスにおける技術と電子商取引を改善することに専念する業界唯一の組織である。BITS の理事会は、米国最大の 14 の銀行持株会社の会長と CEO、およびアメリカ銀行協会(ABA)ならびに Independent Community Bankers of America (ICBA) の代表者で構成される。BITS は、金融産業に対する安全保障研究所の設置が最優先事項であると決定している。

電子銀行業務用のセキュリティ製品をテストする研究所設置のアイデアは、Web ベースの金融取引における成長が現在のように目立つ以前に始まっている。BITS Financial Services Lab が設置されたのは、1999 年 7 月 28 日のことである。この研究所は、BITS と共同で開発され、BITS によって認定された安全保障基準を基に、技術プロバイダの製品やサービスをテストする。BITS の研究所は、新技術の開発やデジタル商取引量の増大に合わせて、金融産業が電子商取引や電子銀行業務に対する安全基準を継続して強化し続けるための 1 つの方法であると見なされている。安全保障研究所の設置はまた、業界が PC バンキングにおける技術危機管理に関する Office of the Comptroller of the Currency (OCC) Bulletin (98-38) の要求を満たす方向に動き出すことが可能であることを示した最も具体的な方法の 1 つでもある。

FS/ISAC

Financial Services 情報共有分析センター(FS/ISAC)は、1999年10月1日に設置された。これは、民間産業がスポンサーとなった最初の情報共有分析センター(ISAC)である。ISACは、金融サービス業界における情報共有のニーズに応える役割を担う。このイニシアチブは、PDD63の要求を満たすとともに、国家の安全保障に関連する懸案事項に対処するため、金融サービス業界が積極的かつ責任のあるイニシアチブを取っていることを連邦政府に示すことになった。さらに重要なのは、業界の利益の安全保障に影響を及ぼす脆弱性、事例、脅威、解決法などに関する最新情報が入手可能になり、そこから生じる利益を得るための手段をISACが金融サービス業界の会員に対して提供できるようになることである。

ISACは、業界の資産に対する脅威、事例、脆弱性や、利用可能な解消法や解決法に関する情報の共有を、認証に基づいて提供するが、場合によっては匿名で提供する信頼性の高いデータベースである。ISACは、インターネットをベースとし、認定された参加者が、金融サービス業界の他の認定会員と情報を安全に共有することを可能にする。政府や情報提供者はデータベースへの入力を提供するが、業界がスポンサーとなっている諮問委員会の個々の承認なしには、会員が提供した情報が政府機関などによって共有されることはない。

入会した参加者は、匿名でデータベースに情報を提供することができる。匿名による情報提供を許可することで、競合する圧力や法的行為の対象となる心配をなくすることができる。提供された情報は、承認されたユーザに提供される前に、ISACによって不適切な部分が削除される。情報は、Webを介する安全で暗号化された接続によって利用可能になる。適当であれば、緊急的な状況や危機的な状況の存在や、追加情報の入手方法などが電子ページでユーザに通知される。また、ユーザ・プロフィールによって通知をフィルタ処理することができるため、参加者の興味の対象となるような事例が発生した場合に参加者にアドバイスを送ることができる。

提供された情報はいずれも、脆弱性やアタックの緊迫度を評価し、組織的な襲撃の可能性を示すパターンを識別するため、分析と安全保障の専門家で構成されたチームによって評価される。この分析チームは、断片を元の状態に復元し、パターンを識別す

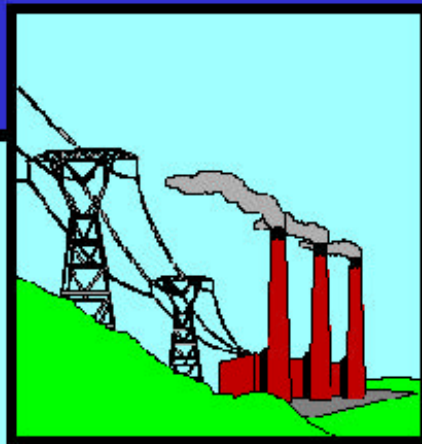
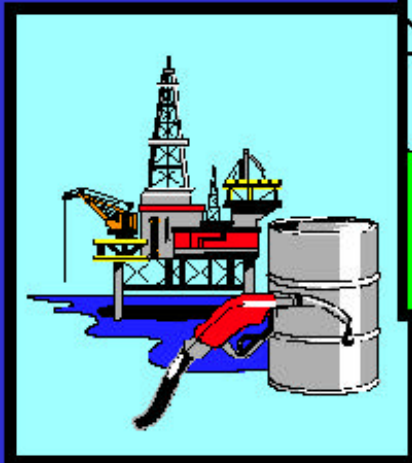
PCCIP と PDD #63 に対する米国政府の対応

るとともに、利用可能な解決法を理解し導入できるよう業界を支援することで、サービスに大きな価値を追加している。



エネルギー部門

重要なインフラストラクチャの生命線



電気
天然ガス
石油

David Jones
局長

重要インフラに関する大統領委員会

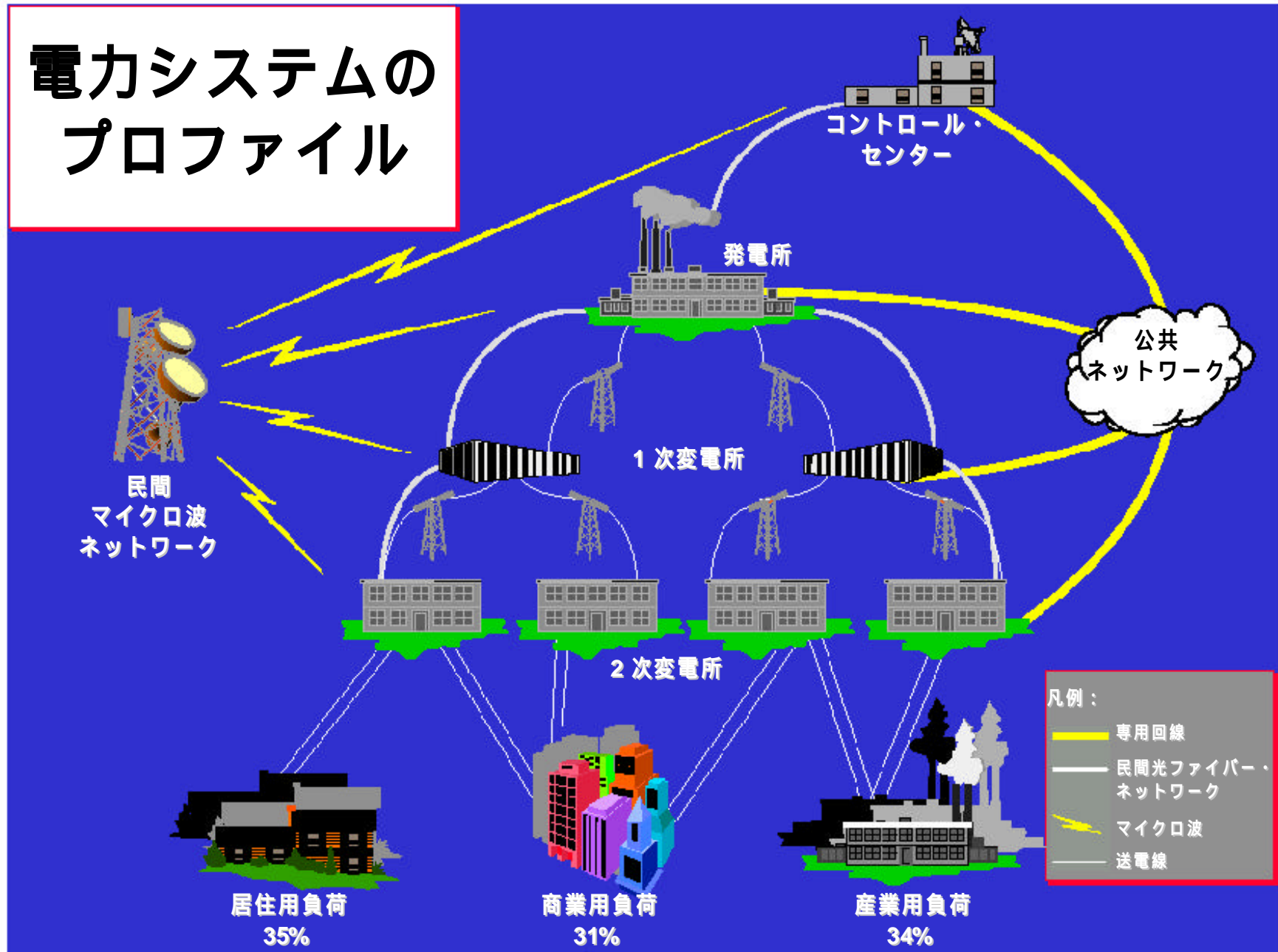
エネルギー

PCCIP は、エネルギーを他のあらゆる部門の「血液」と記している。他のあらゆる部門は、その活動をエネルギーに依存している。エネルギー部門は、電気、石油、および天然ガスの 3 つの産業で構成され、それぞれが独立している。経済的には、この部門の製品の小売は、約 6000 億ドルの収益をもたらしている。

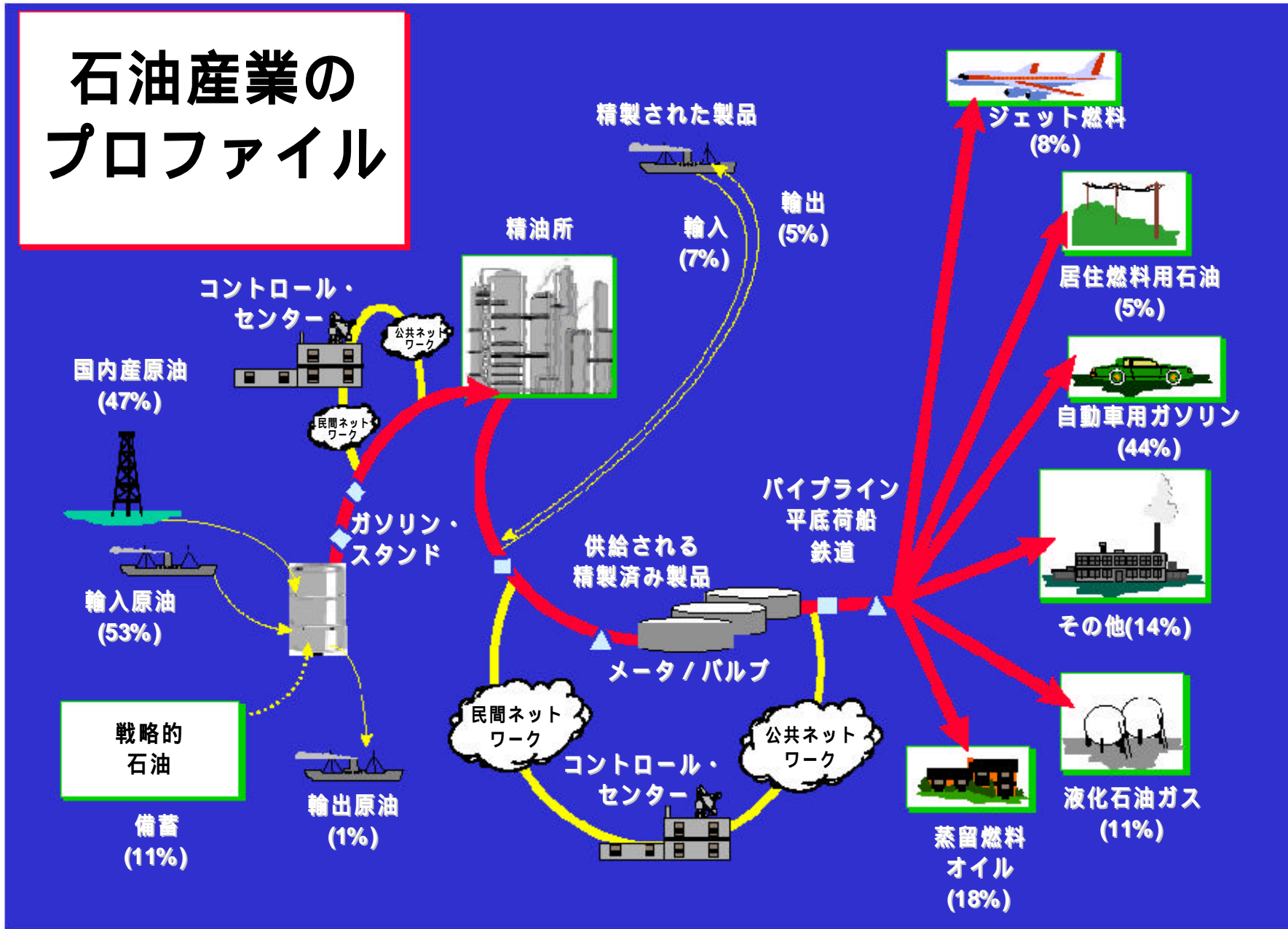
1980 年代、エネルギー部門はエネルギーのインフラストラクチャがテロリストの危険にさらされていることを認識していた。その結果、エネルギー部門は物理的な安全保障を実現するための手段に専念していた。しかし、部門間の相互依存は研究されず、またエネルギー部門における情報システムの急速な普及への準備は行われず、予測もされなかった。しかも、需要が増加する一方で電力の貯蔵は減少している。外国産原油の使用も増加している。これら 2 つの事実は、エネルギー部門の脆弱性を大幅に高めている。いま、エネルギー部門では Supervisory Control and Data Acquisition (SCADA) システムが広く普及している。オープン・システム・アーキテクチャと集中処理を特徴とし、しかも通信の主な手段として公衆通信回線を使用するこのシステムは、サイバー・アタックに対して極めて脆弱になっている。

エネルギー産業は、現時点では Energy ISAC をまだ設置していない。エネルギー産業は、ISAC 用に情報を収集している初期段階にある。米国の電力供給網をサイバー・アタックや物理アタックから確実に保護するため、電力部門のコーディネータとして、電気事業者によって設置された非営利の法人である North American Electric Reliability Council (NERC) が指名されている。National Petroleum Council (NPC) は、米国のエネルギー省に対する諮問委員会である。その目的は、石油や天然ガス、あるいは石油やガス業界に関連する事態について DOE に助言することである。

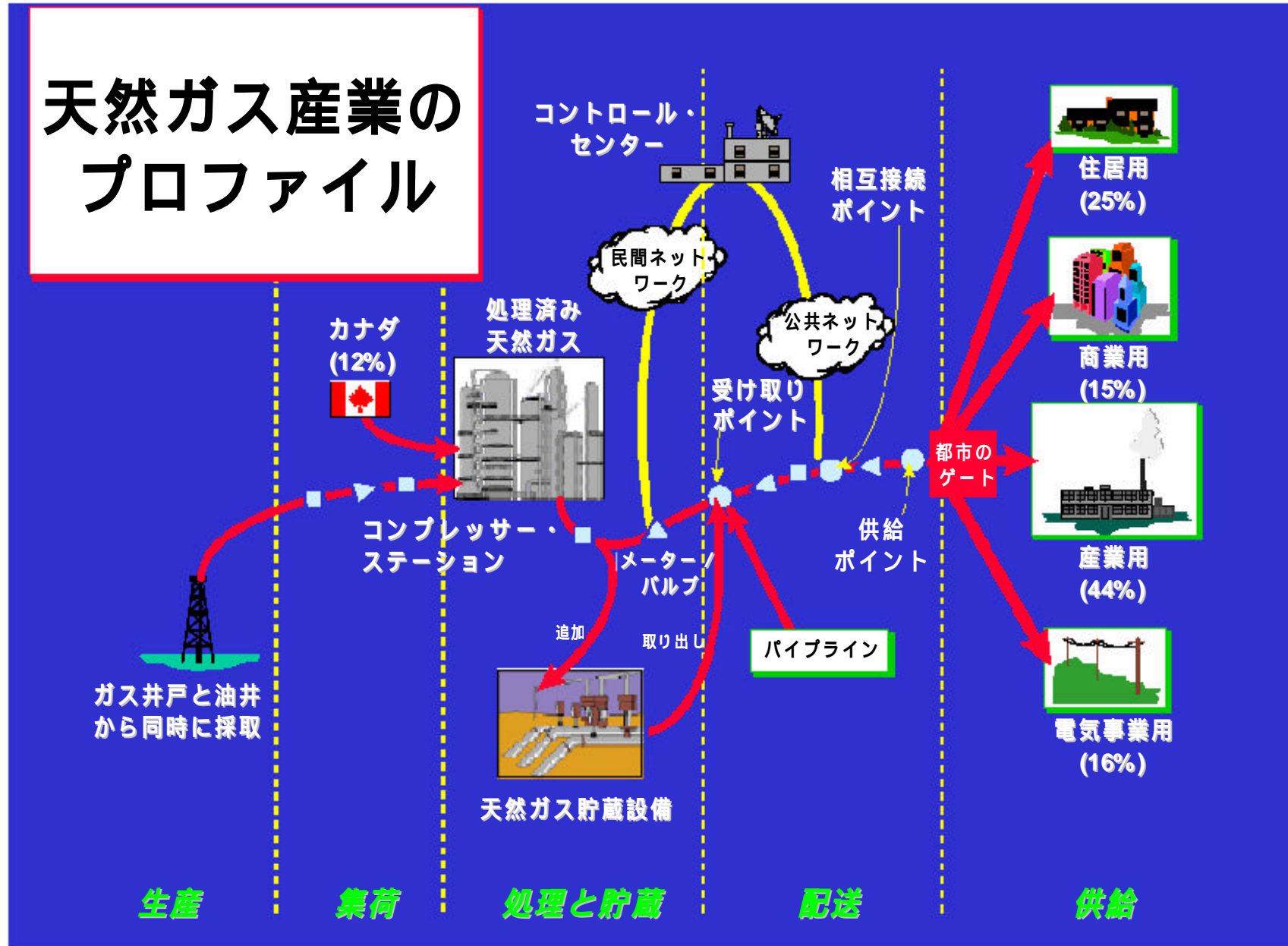
電力システムの プロフィール

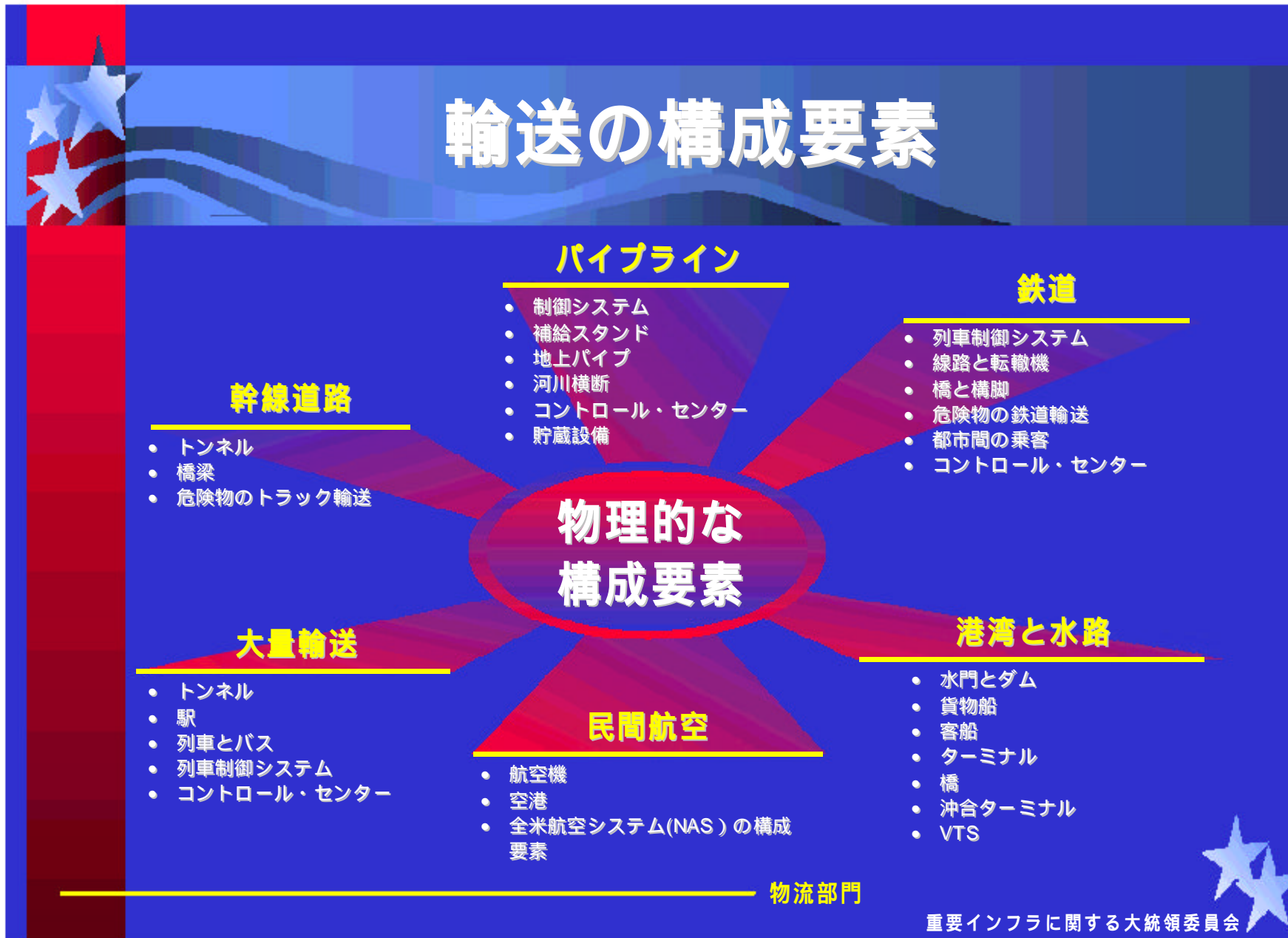


石油産業の プロフィール



天然ガス産業の プロフィール





輸送

PCCIP は、輸送を、商取引、政府の業務、個人的な用事などを支援し実行するため、人や商品のある場所から目的地まで運ぶ航空、鉄道、幹線道路、船舶、水路、および支援システムと定義している。

米国の輸送システムは、ハイウェイ、鉄道、水路、輸送路、パイプラインなどの巨大なネットワークで構成されている。それらに加え、膨大な支援インフラストラクチャが存在する。活動的な輸送システムの数も、増え続けている。また、米国経済の他の部門と同じように、洗練されたコンピュータや通信システムの使用が急増するとともに、それらへの依存が深まっている。輸送は、米国の経済にとって、最も不可欠な部門の一つである。消費者と商品を結びつけるばかりでなく、米国の社会を文字通り動かし続けている。すべてを合わせると、輸送インフラストラクチャの価値は 2 兆 4 千億ドルに達すると評価されている。輸送関連の活動は、米国 GDP のほぼ 20% を占めている。²⁴

しかし、米国の物理的な輸送インフラストラクチャの大半は、寿命や酷使により、早急に修理する必要が生じているのも事実である。また、積み荷の窃盗による損失は、年間 130 億ドルを超える。²⁵ さらに、National Information Infrastructure (NII) に対する依存度が急速に深まったことで、輸送業界は従来の物理的なアタックばかりでなく、サイバー・アタックに対しても防護しなければならなくなった。輸送部門は、テロリストにとって最も目につきやすく、頻繁にその標的になってきたのである。輸送システムに事故が発生すると、その影響は深刻なものになる。飛行機のハイジャックや爆破、飛行機事故、列車事故、石油パイプラインの漏れなどは、輸送システムで事故が発生した場合に、その損失がどれほど大きくなるかをよく示している。

輸送部門の競合企業の多数は、その業務が継続して行われることを保証している。しかし、様々な輸送システムが相互関係と依存度を急速に深めていくなかで、輸送が危険にさらされる機会は増加している。西暦 2010 年までに、GPS(全地球測位システム)が

²⁴ Department of Transportation, "Transportation Physical Infrastructure – Description, Goals and policy Framework", January 1994,

<http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/trd/trd-app.html>

²⁵ TS&T, "Transportation Infrastructure Assurance", 1999

<http://scitech.dot.gov/partech/totaltrm/totalterminal.html>

電波を使用する唯一のナビゲーション方法になるとみられている。Intelligent Transportation System (ITS)などのプログラムは、効率や利益率をたしかに向上させるが、同時に輸送部門をサイバー・アタックに対してより脆弱にする可能性がある。PCCIP の調査によれば、輸送部門はアタックに対する対応や不慮の事故に対する計画をほとんど所有していないことが判明している。また、標準やガイドラインも存在しないに等しい。役割や任務も、明確には定義されていない。National Airspace System が脅威にさらされていないとしても、その遠隔処理システムは、その解放性と冗長性の欠如により、危険にさらされているのである。輸送部門のあらゆる分野において、脆弱性や危機に対する評価を実施しなければならない。また、研究開発をさらに進めることも必要である。情報の共有を促進するとともに、対応や不慮の事故に対する計画を制定することも必要である。

VHS 部門

給水システム



救急サービス

(消防、警察、救急医療)

政府サービス

(連邦、州、地方自治体)



生活必需サービス部門

重要インフラに関する大統領委員会

生活必需サービス

生活必需サービス部門は、給水、救急サービス、政府の継続サービスで構成される。この部門は、製品やサービスが地方自治体、州政府、連邦政府によって所有され、運営されるという点で、他の部門とは異なっている。また、インフラストラクチャにとって必要不可欠ではあるが、他の部門との相互依存度レベルはそれほど高くない。しかし、これらのサービスが崩壊すると、米国民に対して大きなマイナスになる。

給水システム

給水システムには、水源、水源地と貯蔵施設、水路やその他の水輸送システム、濾過洗浄システム、パイプライン、冷却システムや、家庭や産業施設に給水する設備すべてが含まれる。また、廃水処理用や消化用のシステムが含まれる。

大半の米国民は、清潔で豊富な水がいつでも供給されることを当然のことと考えている。しかし、水は事故によって、あるいは意図的に汚染される可能性がある。これは明らかな脆弱性であるが、より可能性が高いのは給水が停止したり、水圧がなくなることである。国民にとって、突然の給水停止は不便なばかりでなく、停止時間が長くなると生活にも重大な影響を及ぼす。しかし、一定レベルの水圧を必要とする消防などのサービスや産業にとっては、給水システムの停止は悲劇的な結果をもたらす可能性がある。給水が完全に停止すれば、農業にも悪影響を及ぼし、重大な経済的結果をもたらしかねない。

救急サービス

救急サービスには、公衆衛生や安全に関する緊急の事件に個人や社会が巻き込まれる場合に呼び出される医療、警察、消防、救助などのシステムと、その隊員が含まれる。

政府の継続サービス

政府の継続サービスには、連邦、州、地方自治体の各レベルにおける業務やサービスで、公衆衛生、安全、福利など、国家のシステムが機能するために不可欠なものが含まれる。

大統領命令により、すべての政府機関には Critical Infrastructure Protection(重要なインフラストラクチャの保護)に責任を持つ高官が任命されている。これらの高官は、必要に

PCCIP と PDD #63 に対する米国政府の対応

じて政策を改善し強化するため、政策を再評価する。また、機関の職員に対してトレーニングを施すとともに、外部の技術的なコンサルティングを利用してテクニカル・アシストを提供する。政府はまた、アタックや事故からシステムを守るため、システムの改善や強化を行うための研究開発費を支払っている。



救急サービス

警察



救急医療



消防

生活必需サービス部門部門

重要インフラに関する大統領委員会

政府サービス

- ◆ アメリカ気象局
- ◆ 移民帰化局
- ◆ 疾病対策センター
- ◆ 社会保障
- ◆ 公衆衛生局
- ◆ 州ならびに地方自治体の支払サービス
- ◆ 公共事業

生活必需サービス部門

重要インフラに関する大統領委員会

付属書類：

公文書

EO 13010

PDD62

PDD63

PCCIP 委員会メンバー略歴

政府の URL および関連サイト

重要財団

EO 13010

大統領命令 EO13010

重要インフラ防衛

1996年7月15日

特定の国家的インフラは極めて重要であり、インフラの機能不全や崩壊は、米国の防衛面や経済面の安全に悪影響を与えられる。この重要インフラとは、通信、電力体系、ガスや原油の備蓄と輸送、銀行や金融、輸送、給水体系、救急サービス（医療、警察、消防および救急など）、および政府の継続性などである。これらの重要インフラに対する脅威は2つのカテゴリーに分類される。すなわち、有形資産に対する脅威（「物理的脅威」）と、これらの重要インフラを制御する情報機器ないし通信機器に対する、電子、無線周波数、あるいはコンピュータに関連した攻撃の脅威（「サイバー的脅威」）である。これら重要インフラの多くは民間セクターが所有、管理しているため、政府と民間セクターが協力して、当該インフラを防衛し、インフラの機能の継続性を保証するための戦略策定が極めて重要である。

したがって、合衆国憲法および諸法規により当方に付与された大統領権限により、以下のように命ずる。

第1節．設置。本項により、重要インフラ防衛に関する大統領委員会（「委員会」）を設置する。

(a) 委員長。連邦政府外部から適任者を大統領が任命する。同委員会の委員長は常勤とする。

(b) メンバー。以下の各行政省庁長官が、2名を上限に委員会の常勤委員を任命する。

- (i) 財務省
- (ii) 法務省
- (iii) 国防総省
- (iv) 商務省
- (v) 運輸省
- (vi) エネルギー省
- (vii) 中央情報局
- (viii) 連邦緊急管理庁
- (ix) 連邦捜査局
- (x) 国家安全保障局

各省庁の被任命人のうち 1 人は、連邦政府外部の個人も可能だが、当該省庁に常勤として雇用される。各被任命人は、運営委員会の承認を得なければならない。

第 2 節 . 長官委員会。委員会は、長官委員会（「長官委員会」）（Principals Committee）を通じて大統領に報告する。長官委員会は、あらゆる報告書ないし推薦状を、大統領に提出される前に査閲する。長官委員会は、以下のメンバーで構成される。

- (i) 財務長官
- (ii) 国防長官
- (iii) 司法長官
- (iv) 商務長官
- (v) 運輸長官
- (vi) エネルギー長官
- (vii) 中央情報局長官
- (viii) 行政管理予算局長
- (ix) 連邦緊急管理庁長官
- (x) 国家安全保障問題担当大統領補佐官
- (xi) 国家安全保障問題担当副大統領補佐官

第 3 節 . 重要インフラ防衛に関する大統領委員会の運営委員会。運営委員会（「運営委員会」）は、長官委員会の代理として委員会の業務を監督する。本運営委員会は、大統領に任命された 4 人のメンバーで構成される。同メンバーのうち 1 人は委員会の委員長に、もう 1 人は大統領事務局(Executive Office of the President)の職員になる。本運営委員会は、委員会の業務の進捗に関する定例報告を受け、長官委員会への諸報告書の提出を承認する。

第 4 節 . 任務。委員会は、(a) 本命令後 30 日以内に本任務の目的に関する陳述を行う。同陳述は、本命令で後ほど述べる包括的目的と、各任務の目的の詳細な提出予定を詳述して運営委員会の承認を得、

(b) (i) インフラ保証を実施、支援、あるいは貢献する公共および民間セクターの各団体、
(ii) 重要インフラの所有者および運営者、および (iii) 議会など、重要インフラ保証問題に利害を有し、これらの問題に関して異なる見通しを有する可能性のある公共および民間セクターのその他の団体と共に行動、協議し、

(c) 重要インフラの不安定な領域と特質、および重要インフラに対する脅威を評価し、

(d) 重要インフラの防衛努力により、どのような法的および政治的諸問題が発生するのかを決定し、これらの問題にどのように取り組むかを評価し、

(e) 包括的国家政策を推奨し、また重要インフラを物理的およびサイバー的脅威から防衛して重要インフラの継続的運用を保証する戦略を遂行し、

(f) 委員会の推奨を行使するために必要な法律ないし規制の改正を提案し、

(g) 随時、運営委員会宛の報告書と推薦状を作成する。但し、最終報告 1 回だけで済ますよう委員会自身を制限してはならない。

第 5 節．重要インフラ防衛に関する大統領委員会の諮問委員会。(a) 委員会は諮問委員会(「諮問委員会」)から助言を得る。本諮問委員会は、大統領により民間セクターから任命された、重要インフラに精通している 10 名を上限とする個人で構成される。本諮問委員会は、委員会の任務の課題に関して、諮問委員会、委員会の委員長、および運営委員会が適切と見なすあらゆる方法で委員会に対して助言を行う。

(b) 委員長は、諮問委員会メンバーから大統領によって任命される。

(c) 本諮問委員会は、改正連邦諮問委員会法(U.S.C.第 5 条適用)に基づき設置される。国防総省は、諮問委員会に関する連邦諮問委員会法の下、議会への報告を除き、共通役務庁が策定した指針と手続きに基づき、大統領の職務を遂行する。

第 6 節．行政。(a) あらゆる行政省庁と諸機関は委員会と協力し、委員会が要求する支援、情報、および委員会に対する助言などを、法律の許容範囲内で提供する。

(b) 委員会と諮問委員会は、公聴会および非公開の聴聞会を開催し、質疑応答を実施し、必要に応じて小委員会を設置することができる。

(c) 諮問委員会メンバーは、諮問委員会に関する業務を無報酬で遂行する。メンバーは、諮問委員会の業務に従事する際は、断続的に公務に従事する人員に関する法律により、特別手当の代わりに日当などの出張手当が認められる。

(d) 国防総省は、法律の許容範囲内、および予算獲得の可能性を条件に、委員会と諮問委員会に行政サービス、人員、その他支援サービス、および必要に応じて職務遂行資金を提供する。また、委員会に代表を派遣している行政省庁の各部門に対しては、その代表の報酬として賠償金を支払う。

(e) 国防総省は、委員会の専門性を論じるために、委員会の要請に基づき、委員会の考察に関して分析、報告、基礎知識やその他の判断材料を提供する非政府系のコンサルタントとサービス契約を締結することができる。さらに、委員会の要請に基づき、行政省庁や諸機関は、現行の諸連邦諮問委員会に対し、法律の許容範囲内で重要インフラ防衛上の諸問題を検討し、助言を行うよう要求する。

(f) 委員会、長官委員会、運営委員会および諮問委員会は、本命令発布日より 1 年で解散する。但し、解散日以前に大統領により延期された場合はこの限りではない。

第 7 節．暫定連携任務。(a) 委員会が分析を実施している間、および大統領が委員会の推薦状を検討し、同状に基づき行動するまでは、地域ないし国家への悪影響があると思われる危機に対処する、あるいは防止するため、既存のインフラ防衛努力の連携を強めることが必要である。本節により、インフラ防衛対策委員会(Infrastructure Protection Task Force)(「IPTF」)を法務省内に設置し、連邦捜査局が委員長を務め、本暫定連携任務を引き受ける。

- (b) IPTF は、既存のいかなるプログラムないし組織も侵害しない。
- (c) 運営委員会が IPTF の職務を監督する。
- (d) IPTF は、連邦捜査局、国防総省および国家安全保障局から最低各 1 人の常勤メンバーを置く。IPTF はまた、他の行政省庁や諸機関からの非常勤メンバーを受け入れる。メンバーは、重要インフラ防衛の分野における専門性に基づき、各省庁や諸機関から任命される。IPTF メンバーの報酬は、メンバーの出身機関や省庁により支払われる。
- (e) IPTF の業務は、連邦政府内外における既存の専門性を見極め、調整することであり、その目的は、
 - (i) 攻撃を察知、防止、中止ないし制限し、業務を回復、復活させるために、専門家の指導を重要インフラに提供、あるいは活用、調整する。
 - (ii) ある脅威に関する情報を事前に入手した場合、警告通知を発行する。
 - (iii) 不安定さを低下させる方法に関する訓練や教育を行い、重要インフラに対する攻撃に対処する。
 - (iv) 将来発生する可能性のある脅威、目標ないし攻撃理論を決定するための事後分析を行う。および、
 - (v) 攻撃を受けている際、あるいは受けた後にあらゆる犯罪捜査を実施するために関連法規の執行当局と連携することである。
- (f) すべての行政省庁および諸機関は、法律の許容範囲内で IPTF と協力し、IPTF が要求する支援、情報および助言を提供する。
- (g) すべての行政省庁および諸機関は、法律の許容範囲内で重要インフラに対する攻撃の脅威、および実際の攻撃に関する情報を IPTF と共有する。
- (h) IPTF は委員会解散後 180 日以内に解散する。但し、解散日以前に大統領により延期された場合はこの限りではない。

第 8 節 . 総則。(a) 本命令は、あらゆる現行法令ないし大統領命令の改正を意図するものではない。(b) 本命令は、ある当事者が米国、諸機関、その職員、ないしあらゆる役職者に対して、法令ないし均衡法で実体上ないし手続き上強制可能なあらゆる権利、恩恵、信託ないし義務の創造を意図するものではない。

1996年7月15日
ホワイトハウス
ウィリアム・J・クリントン
PDD62

1998年5月22日

ファクト・シート

ホワイトハウス
報道担当官事務所
(メリーランド州ミネアポリス)

即時公表用

1998年5月22日

ファクト・シート

テロ撃退：大統領決定指令 62

クリントン大統領は就任以来、テロ対策を最重要国家安全目標としてきた。大統領は、海外の同胞や同志との協力を深め、テロ対策手段としての法令の強制力を強化し、機内や空港での安全向上を図った。これらの努力が奏功し、主要テロリストの攻撃は未然に防止され、多くのテロリストが逮捕され、裁判にかけられて長期投獄を課せられた。それでも米国の無敵の軍事的優位性は、米国への攻撃を選択する潜在的な敵(国家ないしテロリスト集団を問わず)が、通常の軍事攻撃ではなくテロに訴える可能性が高いことを意味する。さらに、先進技術の利用が容易なため、テロリストが壊滅的戦力を利用する可能性が従来以上に高まっている。したがって、敵は、米国の都市に目標を定めて通常と異なる手段、例えば大量破壊兵器を使用し、米国政府の活動を破壊しようとするかも知れない。また、最先端のコンピュータ技術を用いて、米国経済や重要インフラを攻撃しようとするかも知れない。

クリントン大統領は、来世紀の米国は当該テロリストの攻撃を遅らせ、防止できるようにしたいと決意している。大統領は、当該攻撃が発生した場合には、損害を限定させ、結果を処理する能力も備えなければならないと確信している。

これらの課題を解決するため、クリントン大統領は大統領決定指令 62 に署名した。本指令では、来世紀のテロリストの脅威と戦うための新しく一段と組織的なアプローチが策定されている。本指令は、テロ撃退における役割を課せられている多くの米国諸機関の任務を強化している。また、米国のテロ対策は、テロリストの逮捕、起訴から、輸送機関の安全性の向上や反応力の強化、米国経済の心臓部に位置するコンピュータベースのシステムの防御に至るまで広範であるが、本指令は、このテロ対策における諸機関の活動を分類し、明白に規定している。本指令は、今世紀に遭遇した軍事的脅威と同様の厳格さを持って 21 世紀のテロ脅威に対処するという大統領の目標達成の一助となる。

国家調整役

このテロ対策における新たな統合水準を達成するため、PDD-62 に基づき、安全、インフラ防衛およびテロ対策のための国家調整役事務局(Office of the National Coordination)が開設される。国家調整役は、広範な関連警察機構やプログラム(たとえば、テロ対策、重要インフラ防衛、軍備、および大量破壊兵器の重要性管理などの分野)を監督することになる。国家調整役は、国家安全保障会議に勤務し、国家安全保障問題担当大統領補佐官を通して大統領に報告を行い、大統領のために安全保障軍備年次報告書を作成する予定である。国家調整役はまた、テロ対策プログラムの予算に関する助言を行い、率先して危機管理に必要なと思われる指針の策定にあたる。

PDD63

白書

重要インフラ防衛に関するクリントン政権の政策：

大統領決定指令 63

1998年5月22日

本白書は、クリントン政権の重要インフラ防衛に関する政策の主要部分を説明するものである。本白書は、公共、民間両セクターのすべての利害関係者への普及を目的としている。また、国防大学や国家外務訓練センター(National Foreign Affairs Training Center)などの米国政府系専門教育機関において、諸省庁間の実務や手続きに関する授業や演習においても使用される予定である。米国政府のあらゆる省庁が、この機密扱いされていない白書が広範に普及することを奨励している。

・ 潜在的不安定性の増加

米国は、世界最強の軍隊と最大規模の経済の両方を保有している。このような米国の国力の2つの側面は、相互に強化し合いながらも独立している。また、双方とも特定の重要インフラとサイバーベースの情報システムに一段と依存している。

重要インフラは、米国経済や政府の最低限の運営にとって不可欠な、物理的でサイバーベースのシステムである。重要インフラとは、たとえば、政府および民間の両セクターにおける通信、エネルギー、銀行や金融、輸送、上水道、および緊急サービスなどである。国家の重要インフラは歴史的に、物理的にも論理的にも独立したシステムで、相互依存性はほとんどなかった。しかしながら、情報技術の進歩や効率性向上の必要性が高まった結果、これらのインフラは一段と自動化され、連結されてきた。これらの同時進歩により、機器の誤作動、人的ミス、天候やその他の自然災害、および物理的攻撃やサイバー攻撃に対する不安定性が新たに露呈するようになった。このような不安定性と取り組むことにより、公共民間両セクターに及び、国内外両面の安全性を防衛する、柔軟で革新的なアプローチが必然的に必要になる。

米軍は最強であるため、今後の敵は、国家やグループ、個人に関わらず、通常と異なる方法、たとえば米国内における攻撃などにより米国に打撃を与えようとするかも知れない。米国経済は、相互依存性とコンピュータ化されたインフラに一段と依存しており、米国のインフラと情報システムに対する通常と異なる攻撃は、米国の軍事力と経済の両面に大規模な打撃を与える能力を有しているかも知れない。

・ 大統領の意図

重要インフラの継続性と存続性を保障することは、米国の長年の政策であった。クリントン大統領は、米国はあらゆる必要な手段を講じ、米国の重要インフラ、特に米国のサイバーシステムに対する物理的およびサイバー攻撃の両方に対する不安定性を速やかに排除したい考えである。

・ 国家目標

米国は、2000 年までに当初の運用能力を達成し、大統領決定指令 63 に対する大統領の署名日から遅くとも 5 年以内に、以下のような能力に大幅な打撃を与えられる意図的行為から当国家の重要インフラを防衛する能力を獲得し、維持する。

- 重大な国家安全保障任務を遂行し、総合的な公衆衛生と公的安全を保障する連邦政府の能力
- 命令を遵守し、最低限の重要な公益事業を供給する州政府や地方自治体の能力
- 秩序ある経済の機能と、重要な通信、エネルギー、金融および輸送サービスの提供を保障する民間セクターの能力

これらの重要な機能のいかなる妨害ないし操作も、一時的なもので、希にしか発生せず、管理可能で、地理的に孤立したもので、米国の福祉にとっての不利益が最小限に留まっていなければならない。

・ 不安定性を低下させる公共と民間の提携

経済および政府の施設は共に、米国の重要インフラに対する攻撃目標になりそうなたため、米国の潜在的な不安定性を排除するには、公共および民間セクター双方の緊密な調整努力が必要である。成功するためには、この提携関係が真正で、相互的であり協力的なものであることが必要である。したがって、米国の重要インフラの不安定性を排除するという国家目標を達成するに際しては、米国政府は予測可能な限り、民間セクターに対する政府の規制が増加する、あるいは資金が調達されていない政府の権限を拡大させる結果を避けなければならない。

インフラへの攻撃に対して不安定な米国経済の各主要セクターのために、連邦政府は指定主要機関から上級高官を 1 名、民間セクターと協力するセクター連絡職員として任命する。セクター連絡職員は、当該セクターの民間企業との協議、調整後、同セクターを代表する民間セクターの相手方(セクター調整役)1 人を認定する。この 2 人と、2 人が代

表する省庁および企業は共に、以下の行為によりセクターの全米インフラ保証計画に貢献する。

- サイバーないし物理的攻撃に対する当該セクターの不安定性を評価する。
- 重大な不安定性を排除する計画を推奨する。
- 大規模な攻撃計画を認定し、防止するシステムを提案する。
- 進行中の攻撃を警告、牽制、阻止する計画を策定し、その次に必要に応じて FEMA と連携し、攻撃の影響が残る中、最低限必要な機能を速やかに再組成する。

セクター計画の準備期間中、国家調整役(第 6 節参照)は、主要機関セクター連絡職員および国家経済会議の代表と共に、相互依存性に特定の焦点を当てながら、各代表の全体的調整と多様なセクター計画の統合を確実に行うものとする。

. 指針

この潜在的な不安定性と、当該不安定性の排除手段に取り組むに際し、クリントン大統領は当該関係者が、以下の一般的な原則と問題に注意を払うことを望んでいる。

- 我々は、本指令に規定する目的を達成するためのアプローチとプログラムに関し、議会と協議し、議会からの投入を要求する。
- 米国の重要インフラ防衛は、必然的に所有者、運営者および政府間で責任を分担するものである。さらに、連邦政府は国際協力を奨励し、一段と国際化する本問題への対応を支援する。
- 米国の重要インフラの現在の信頼性、不安定性および環境の脅威は、評価を頻繁に行う。その理由は、科学技術や重要インフラに対する脅威の本質が急速に変化し続けており、米国の防衛手段や対応を強力的に適合させる必要があるためである。
- 市場が提供するインセンティブは、重要インフラ防衛問題を提起する最初の選択肢である。規制の利用は、米国民の衛生、安全ないし安寧の防衛に失敗するという、市場の重大な過失に直面した場合に限られるであろう。そのような場合、諸機関は、規制の監督に利用できる選択肢を認定し、評価する。たとえば、望ましい行為を奨励するための経済的インセンティブの提供や、民間セクターが選択肢を作成する原因となる諜報の提供などである。当該インセンティブは、その他の行為と共に、最先端の科学技術を利用する一助となり、民間セクターの所有者や運営業者が最大限実行できる安全性を獲得し、維持できるように策定する。
- 法の執行、規制、海外情報の収集、軍備などすべての政府の権限、能力および人材は、適時利用可能であり、重要インフラ防衛の達成と維持を保障する。

- プライバシーの尊重には、注意を払わなければならない。消費者と運用業者は、情報が正確に、内密にそして信頼できる水準で取り扱われることに信頼をおく必要がある。
- 連邦政府は、調査、開発および調達を通して、一段と有効なインフラ防衛手段の導入を奨励する。
- 連邦政府は、インフラ保障の最善の達成法に関するモデルとして民間セクターに奉仕し、実行可能な範囲内で、努力の結果を同セクターに知らせる。
- 我々は、脅威や危機管理だけでなく、防止策にも焦点を当てなければならない。その限りにおいて、民間セクターの所有者や運用業者は、自身が管理するインフラのために実現可能な最大限の保障を提供し、当該業務において支援材料となるような情報を政府に提供しよう奨励されるであろう。民間セクターに完全に従事するためには、所有者と運用業者の全米インフラ防衛システムへの自発的参加が望まれる。
- 力強く柔軟なインフラ防衛プログラムには、州政府および地方自治体と、最初の回答者との間の緊密な協力と連携が不可欠である。あらゆる重要インフラ防衛計画と行動には、州政府および地方自治体と最初の回答者のニーズ、活動および責任が考慮される。

・ 組織の機構

連邦政府は、以下の 4 つの構成要素(別紙 A で詳述)周辺で努力することを目的として組織される予定である。

1. セクター連絡担当主要機関：大規模なサイバーないし物理的攻撃の目標になる可能性がある各インフラセクターのために、米国政府の一部署が連絡のための主要機関になる予定である。各主要機関は、当該分野のセクター連絡職員になり、重要インフラ防衛関連の諸問題への取り組み、および特に、全米インフラ保障計画の部局の推奨において、民間セクターの代表(セクター調整役)と協力する、副長官以上のクラスの人間を 1 名任命する。同時に、主要機関と民間セクターの相手方は、各々のセクターのために、不安定性認識教育プログラムを策定し、実行する。
2. 特別任務担当主要機関(Lead Agencies for Special Function)：さらに、主に連邦政府が実践しなければならない重要インフラ防衛関連の特定任務(国防、外務、諜報、法の執行)がある。各当該特別任務のために、米国政府の当該分野におけるあらゆる行動を責任を

もって調整する主要機関が存在する。各主要機関は副長官以上のクラスの上級高官 1 名を、連邦政府の当該任務の任務調整役として任命する。

3. 省庁間調整：主要機関のセクター連絡職員および任務調整役は、国家経済会議などの他の関連行政省庁や諸機関の代表同様、安全、インフラ防衛およびテロ対策担当国家調整役が委員長を務める重要インフラ調整グループ(CICG)の支援下で会合を開き、本指令の実行を調整する。本国家調整役は大統領によって任命され、国家安全保障問題担当大統領補佐を通して大統領に報告する。同補佐は、経済問題担当大統領補佐との適切な調整を保障する。CICG に派遣される機関の代表は、上級高官(補佐官以上)である。CICG は適時、安全政策委員会、安全政策フォーラムおよび国家安全および通信、情報システム安全委員会など、現行の政策機構によって支援される。

4. 全米インフラ保障委員会(National Infrastructure Assurance Council)：主要諸機関、国家経済会議および国家調整役の推薦に基づき、大統領は、大手インフラ提供者と地方自治体高官の専門委員団を全米インフラ保障委員会に任命する。委員長は、大統領が任命する。国家調整役は、委員会の執行取締役として業務を遂行する。本全米インフラ保障委員会は定期的に会合を開催して米国の重要インフラ防衛における公共と民間セクターの協力関係強化を図り、大統領に適時報告書を提出する。連邦政府上級高官は、全米インフラ保障委員会(National Infrastructure Assurance Council)会議に適時参加する。

・ 連邦政府重要インフラ防衛

連邦政府の行政省庁および諸機関は、政府自身の重要インフラ、特にサイバーベースのシステムの防衛責任を有する。各行政省庁および諸機関の最高情報責任者(CIO)は情報の保証に責任を有する。各行政省庁および諸機関は、自身が所有する重要インフラのあらゆるその他の側面に防衛責任を有する最高情報保証責任者(CAO)を任命する。各部署の裁量により、CIO が CIAO を兼任することもできる。これらの責任者は、政府のコンピュータや物理的システムの不安定性評価を実施するための、適正で正当な委任手続きを確立する。法務省は、当該委任実施のための法的指針を策定する。

本指令発布後 180 日以内に、各行政省庁および諸機関は、自身が所有する重要インフラの防衛計画を策定する。国家調整役は、行政省庁および諸機関の政府間依存と、当該依存の解消により必要となった調整分析に責任を有する。重要インフラ調整グループ(CICG)は、当該計画の専門的見直し手続きを主催する。当該計画は、本日より 2 年以内に実行し、2 年毎に見直す。この計画に基づき、連邦政府は民間セクターに最善の重要インフラ防衛策のモデルを提示する。

・ 任務

長官委員会は、以下の付随的な関連任務の段階的な達成目標を記載した全米インフラ保証計画の実行予定表を、本指令発布後 180 日以内に大統領に提出しなければならない。

1. 不安定性分析：米国への大打撃を意図したインフラ攻撃目標の一つと思われる米国経済および政府の各セクターのために、最初に不安定性の評価を行い、その後定期的な見直しを行う。この評価には、各セクターの最低限重要なインフラを決定することも適宜含まれる。
2. 救済計画：不安定性分析に基づくと、望ましい救済計画が必要になる。本計画は、実行予定、責任および資金調達に関して規定する。
3. 警告：大規模なインフラ攻撃を警告する全米センターを早急に設立する(別紙 A 参照)。その後速やかに、民間セクターの可能な限り最大限の参加を得て当該攻撃を検知、分析する高度システムを配備する。
4. 対応：大規模なインフラ攻撃の最中に対応するシステムには、被害を遮断し、最小化するという目標がある。
5. 再組成：多様な水準のインフラ攻撃に備え、必要最小限の能力を速やかに再組成するシステムを備える。
6. 教育と認識：安全性の重要度に対する感度を高め、特にサイバーシステムに関する安全基準において関係者を訓練する不安定性認識教育プログラムを、政府および民間の両セクターに備える。
7. 研究開発：インフラ防衛を支援するため、連邦政府が支援して研究開発を実施する。同研究開発は、複数年に渡って計画されることが必要で、民間セクターの調査を考慮し、十分な資金を投入して、早急だが達成可能な計画に基づき米国の不安定性を極小化する。
8. 諜報：諜報共同体(Intelligence Community)は、我が国の国家的インフラに対する諸外国の脅威に関する情報の収集と分析の強化計画を策定し、実行する。この情報は、海外のサイバー / 情報戦争の脅威の例に限定されない。
9. 国際協力：同様の志向を持つ友好国、国際組織および多国籍企業との重要インフラ防衛協力の拡大計画を策定する。
10. 立法上および予算面での必要事項：重要インフラに関する行政省庁の立法当局および予算面での優先度を評価する。また、必要に応じ、大統領に改善に役立つ進言を行う。この評価および進言を行う場合は、OMB の役員と調整する。CICG はまた、別紙 B に記載する任務の遂行を検討し、予定を組む。

・ 実行

国家調整役は、180 日報告書の他に、国家経済会議(National Economic Council)と協力して本指令の実行に関する年次報告書を、国家安全保障問題担当大統領補佐を通して大統領と行政省庁および諸機関の責任者に提出する。本報告書には、脅威に関する最新の評価、国家計画用に設定された段階的目標の達成状況報告、および追加政策、法律面および予算面からの進言などを盛り込まなければならない。この評価および進言を行う場合は、OMB の役員と調整する。さらに、2000 年の初期運営能力の確立後、国家調整役はゼロ・ベースの検討を実施する。

別紙 A： 機構および組織主要機関： 特定セクターおよび特定任務には、米国政府内での
明白な説明義務が示される必要がある。以下のように責任を付与する。

セクター連絡担当主要機関：

商務省	情報および通信
財務省	銀行および金融
環境保護局	給水体系 航空 高速道路(トラック輸送およびインテリジェント交通システムなど)
運輸省	大量輸送 パイプライン 鉄道 海上貿易
法務省 / FBI	緊急法執行業務
FEMA	緊急消火業務 公共サービスの継続性
厚生省	公衆衛生サービス(予防、監視、研究所業務および個人衛生サービス)
エネルギー	電力 原油およびガス製造備蓄

特別任務担当主要機関：

法務省 / FBI	法執行および国内治安業務
CIA	海外諜報
州外務	
国防省	国防

さらに、OSTP は、全米科学技術委員会(National Science and Technology Council)を通じた研究開発課題と政府用プログラムの調整に責任を有する。また、商務省は情報通信の主要機関であり、国防省は、米国通信システムと、大統領の国家安全保障データ通信諮問委員会の支援に執行代理責任を有する予定である。

国家調整役：安全保障、インフラ防衛およびテロ対策担当の国家調整役は、本指令の実行に関する調整責任を有する。国家調整役は、国家安全保障問題担当大統領補佐を通じて大統領に報告を行う。同調整役はまた、インフラ問題を検討するために副長官ないし長官委員会会議が開催される際は、常任メンバーとして参加する。全米調整役は、行政省庁および諸機関を監督しないものの、政策の策定および実行のために省庁間の調整を確実にし、大規模な海外との関与を伴うインフラ関連の危機対策活動を検討する。国家調整役は、策定済みの年間予算計画に従い、機関の重要インフラ防衛予算に関して助言を行う。国家調整役は重要インフラ調整グループ(CICG)の委員長を務め、副長官委員会(あるいは、委員長の要請があれば長官委員会)に報告する。セクター連絡職員および特別任務調整役は、CICG 会議に出席する。行政省庁および諸機関は各々、同会議に常時出席する CICG 上級高官(補佐官クラス以上)を任命する。国家安全保障局は、NSC 職員からインフラ防衛担当取締役を 1 名任命する。

国家計画調整(NPC)の職員は、法律に従い、行政省庁および諸機関から復帰することのないベースで完全に転籍する。NPC 職員は、様々なセクター計画を統合して全米インフラ保証計画を策定し、米国政府自身の重要インフラに対する依存性分析を調整する。NPC 職員はまた、全米教育認識プログラムと、法的および公的諸問題の調整を援助する。国防省は 98 年度中、NPC の基幹を成す任務移行局の執行機関として引き続き業務を遂行する。NPC は、99 年度からは商務省の一部になる。人事管理庁は、NPC の業務の遂行に対し、必要な援助を行う。NPC は、大統領指令で延期されない限り、01 年度に終了する。

警告情報センター 全米警告情報共有制度の一環として、大統領は早急に FBI に代理権を付与し、現行組織を大規模な全米インフラ防衛センター(NIPC)に拡大する。本組織は、国家的重要インフラに対する脅威の評価、警告、不安定性および法の強制力の調査、および対応を行う団体として業務を遂行する。大統領はまた、当初の 6 ヶ月から 1 年間、セクター調整役、特別任務調整役および国家経済会議の代表と協力して、国家調整役およびセクター連絡職員に対し、重要インフラの所有者および運用業者と協議し、下記のような民間セクター共有分析センターの設立を奨励するよう適宜指示する。

全米インフラ防衛センター(National Infrastructure Protection Center) (NIPC) : NIPC には、国防総省、諜報団体および主要機関から就任している代表に加え、FBI、USSS およびコンピュータ犯罪やインフラ防衛に経験を有するその他の調査機関などが含まれる予定である。NIPC は、あらゆる民間セクター共有分析センターだけでなく、他の警告管理センターなどの連邦政府の他機関と電子的に連結される。NIPC の使命は、適時の国際的脅威の警告、包括的分析および法強制力調査および対応などである。

あらゆる行政省庁および諸機関は、NIPC と協力し、NIPC が要請する可能性のある援助、情報および助言を、法律の許容範囲内で提供する。あらゆる行政省庁はまた、NIPC と、政府および民間セクターの重要インフラへの脅威や攻撃の警告、実際の攻撃に関する情報を NIPC と共有する。NIPC には、警告、分析、コンピュータ調査、非常時の対応の調整、訓練、救済活動および専門技術の開発と応用に責任を有する部署が開設される予定である。さらに、NIPC は、民間セクターの他団体や、民間セクターが設立する可能性のあるあらゆる情報共有分析団体(例えば、下記の情報共有分析センターなど)との間に独自の直接的関係を構築する。

NIPC は、情報発信機関と共に、同センターが関連の連邦政府や州政府の諸機関、地方自治体(すなわち重要インフラの所有者や運用業者)、およびあらゆる民間セクターの情報共有分析団体宛に提供する分析や報告書に挿入するため、法の執行や諜報を適切な形態に調整する。情報団体から発信された国家安全に関する情報やその他を伝達する前に、NIPC は従来の手続きに従って情報団体と全面的に調整する。調整済み、ないし未調整報告に関わらず、NIPC は、脅威的状况の悪化に関する攻撃警報ないし注意報を、あらゆる民間セクター情報共有分析団体とインフラの所有者や運用業者に発令する予定である。これらの警報にはまた、所有者や運用業者が採るべき追加的防衛策に関する指針が含まれる。極度の非常事態を除き、NIPC は国家調整役との調整後に、国際テロリスト、諸外国ないしその他の敵意を持った海外権力による急迫の攻撃に関し、警報を発令する。NIPC は、インフラへの脅威に関する情報の収集拠点を全米に設ける。さらに、NIPC は、事変に対する連邦政府の反応の助長および調整、攻撃の緩和、脅威の調査および再組成努力の監視を行う重要な手段を提供する。海外からの脅威 / 攻撃の質と水準、特別任務機関(DOJ/DOD/CIA)間で策定された議定書、および大統領の最終決定によって、NIPC は DOD ないし諜報委員会のいずれかを直接支援する立場に置かれる可能性がある。

情報共有分析センター(Information Sharing and Analysis Center) (ISAC) : 国家調整役は、セクター調整役、セクター連絡職員および国家経済会議と協力し、民間セクターの情報共有分析センター設立を強力的に奨励するため、重要インフラの所有者および運用業者と協

議する。同センターの実際の構想や職務と、NIPC との関連性は、民間セクターが連邦政府との協議と助力を得て決定する。国家調整役は、本指令より 180 日以内に国家経済会議などの CIG の支援を受け、ISAC の設立に奏功する連邦政府の助力を得る方法を策定する。

当該セクターは、産業界および NIPC の両方に対し、民間セクターの情報の収集、分析、適切な整理および伝達を行うための機構として機能する可能性がある。同センターはまた、民間セクターに情報を追加提供するため、NIPC からの情報の収集、分析および伝達を行う場合もある。この不安定性、脅威、侵害行為および異常事態に関する重要情報の共有機構は、政府と産業界の協力関係にとって重大である一方、企業と政府間の直接的情報交換に關与するものではない。民間セクターの代表が最終的に意図しているとおり、ISAC は、特に民間と非政府セクターの幅広い相互交換が極めて成果を上げていると証明された疾病制御予防センターなどの施設に、ある側面では対抗することが可能である。

ISAC は、当該モデル下で大規模な技術集中や専門知識と、非法規的で違法な執行任務を獲得するであろう。ISAC は、自身や政府が適切と見なしているように、様々なインフラに関する基本的統計やパターンを確立し、多様なセクター内かつセクター間の情報交換センターとなり、民間セクターが利用する過去のデータの蓄積を提供すると思われる。当該施設の成功にとって重大なことは、適時性、利便性、調整、柔軟性、有益性および許容性であろう。

別紙 B：追加任務調査：国家調整役は、以下の項目に関する調査を委任する。

- 民間セクターの企業が情報共有に参加することにより生じる責任問題
- 情報共有に対する既存の法的障害。当該障害の撤廃要求、たとえば、米国の法的機関との協力によるモデルコードの立案を通じたものなどを目的とする。
- 脅威や不安定性に関する情報を誤用する人物への開示、ないし受け入れ難い開示リスクを回避する一方、当該情報を確実に共有できる方法や情報システムに加え、文書や情報の分類の必要性和、当該分類が有益な情報伝達に与えるインパクト
- 確実な情報伝達や情報操作システムなど、産業界の取引上の機密やその他の業務上の機密データ、法の執行に関する情報および証拠資料の防衛の強化、分類済みの国家安全情報、民間セクターが所有するインフラの不安定性を開示している未分類の資料、および一見して無害の情報など、総体的に開示が賢明でないもの

- 米国のインフラの安全性には情報の共有が必要と見なしている海外の団体との情報共有の内容
- 次の行為を行う際の安全基準に対する潜在的恩恵。権限委譲、助成、あるいは選別された重要インフラ提供者に保険を提供する際の支援、および米国とのビジネスを希望する海外の重要インフラ提供者のための保険の抱き合わせ要求。

公的救済活動 インフラ防衛問題に対する政府の向上した敏感度を判断するため、以下の行為を行う。

- 国家調整役の監視下にあるホワイトハウスは、関連閣議機関と協力し、以下の一連の会議を検討する。(1) 政府と民間セクターの有力指導者を召集し、情報安全保障に対する委任の増加プログラムを提案する会議。(2) エンジニアリング、コンピュータ科学、ビジネスおよびロー・スクールから学会の有力者を召集して情報安全保障教育の状況を見直し、将来は、本分野の専門家に対する国家的要求を満たすために必要なカリキュラムや人材の変化を認知する会議。(3) コンピュータ倫理周辺の諸問題に関する会議。これは、本問題が、K から 12 まで、および一般的な大学の生徒数に関連するため。
- 科学アカデミーと技術アカデミーが円卓会議を考慮し、連邦政府、州政府および地方自治体の高官と、産業界および学会の指導者が、インフラ安全保障を強化する国家戦略を策定する。
- 情報団体と法の執行機関は、インフラ所有者および運用業者と、政府の上級高官に事情説明を行うため、既存のプログラムを拡大する。
- 国家調整役は、(1) 政府および民間の上級高官と共に、インフラ保障シミュレーション用プログラムを策定するものとし、同プログラムの報告書はキャンペーン認知の一環として配布されることがある。(2) 民間セクターと連携し、継続的な全米規模の認知キャンペーンを始動し、インフラの安全性が向上していることを強調する。

連邦政府内の行動 連邦政府が自身のインフラの安全性の向上を図るため、以下のような手段を早急に講じる。

- 商務省、共通役務庁および国防総省は、連邦政府の諸機関を支援し、各機関内の情報保障の最善策を講じる。
- 国家調整役は、情報保障という課題を課せられた現在の連邦政府、州政府および地方自治体を見直し、これらの諸機関がいかに効果的に協力できるかに関して提言を行う。

- あらゆる連邦政府の諸機関は、自身のコンピュータシステムにアクセスする権限を付与できる人物を明白に任命する。
- 情報団体は、米国の重要インフラに脅威となる海外のサイバー / 情報戦争に関する情報の収集と分析強化の重要性を高め、形式化する。
- 連邦捜査局、シークレット・サービスおよびその他の適切な諸機関は、(1) 地元
のコンピュータ犯罪対策グループと共に、卒業前および卒業予定で、関連するコ
ンピュータ関係の技能を有する生徒を常勤および非常勤の社員として採用する活
動を精力的に展開し、(2) サイバー攻撃に関連したテクニカル分析や調査に才能
を持つ人材を雇用し、確保する。
- 運輸省は、国防総省と協議し、GPS(全地球測位システム)に依存する全米の輸送
インフラの不安定性を徹底的に評価する。本評価は、GPS ベースのシステムの
一般ユーザーに対するリスクの独立した統合評価を保障するほか、このような評
価に基づいて近代化された NAS の最終構造に関する決定を下すとの見方を備え
ている。
- 連邦航空局は、包括的な航空宇宙システム安全保障プログラムを開発、実行し、
近代化した NAS を、情報をベースにしたものやその他の破壊および攻撃から防
衛する。
- GSA は、インフラ保障に関連した大規模な調達(新連邦通信システム)を認定して
本調達の過程がインフラ防衛の重要度を反映しているか否かを調査し、必要に応
じて全体的な調達過程の見直しを提案する。
- OMB は、連邦諸機関に対し、任命されたインフラ保障業務を政府実績および結
果法の戦略計画および実績測定体制に含めるよう指示する。
- NSA は、NSD-42 中の全米管理者責任に準じ、米国政府のシステム調査を包含す
る評価の実践、脅威と不安定性に関する情報の伝達、基準の設定、研究開発、お
よび問題安全製品の評価を行う。

民間セクターの支援 民間セクターによるインフラの安全性の達成および維持を支援す
るため、

- 国家調整役と全米インフラ保障委員会は、民間業界が情報や通信システムなどの
重要資産に対して実践する定期的リスク評価を奨励する方法を提案、策定する。
- 商務省と国防総省は協力し、民間セクターと連携しながら、専門知識を民間セク
ターの重要インフラ所有者や運用業者に提供し、最良の安全保障関連の実践基準
を策定する。

PCCIP と PDD #63 に対する米国政府の対応

- 法務省と財務省は包括的調査を支援して、コンピュータ犯罪件数統計の編纂、コンピュータ犯罪に対する国家のアプローチの比較、および青少年によるコンピュータ犯罪の防止、対応策の策定を行う。

PCCIP 委員会メンバー略歴

委員長

ロバート T. マーシュ(Robert T. Marsh)

重要インフラ防衛に関する大統領委員会委員長

宇宙開発コンサルタントであるマーシュ氏は、現在 CAE エレクトロニクス社およびコンバース・ガバメント・システム社会長、テクノリッジ社取締役、ならびに MITRE 社管財人を務め、また米空軍エイド・ソサエティの指揮官を務める。1989-91 年にチオコール社初代会長に就任する前は、空軍システム司令部指令官として空軍向け宇宙開発システムの調査、開発、テスト、および捕捉を指揮、1984 年に米空軍大將を退役した。

委員会メンバー

メリット・アダムス(Merritt Adams)

アメリカン・テレフォン・アンド・テレグラフ(AT&T)

国際的な情報通信コンサルタントであるアダムス氏は、エレクトロニック・サーベイランス、通信保護手段の開発、ソフトウェアの研究開発を専門とする。[AT&T](#)では 35 年間に渡り、国際的な交換機ビジネス部門において世界規模で展開する新ビジネスの開発に役員として携わる。この経験と専門技術を有する同氏は、委員会の電子分配システムチームに不可欠な人材である。

リチャード P. ケース(Richard P. Case)

インターナショナル・ビジネス・マシズ(IBM)

シーズ氏は、IBM 社員の技術戦略開発の取締役として従事。同氏の IBM における 41 年間の経験は委員会にとって貴重な技術知識であり、その分野はハードウェア、ソフトウェア、半導体開発、システム構築、研究所管理、訴訟、ならびに人事管理などに渡る。同氏は、マスカウント基金管財人、コンピュータ・ミュージアム副館長を務め、専門技術者ライセンスを有する。委員会では、国家体系チームおよび電子分配システムで活躍。

メアリー・J.カルナン博士(Mary J. Culnan)

ジョージタウン大学

カルナン氏は、ジョージタウン大学ビジネススクールで助教授を務め、現在は休職中。ジョージタウンで情報システムおよび電子商取引の講義、ならびに電子市場で発生した消費者プライバシーの問題に関して調査を行っている。委員会では公的信頼感チームでリーダーを務め、情報通信チーム、銀行・財政チーム、グローバルチームで活躍。カルナン助教授は連邦議会で一連のプライバシー問題に関する証言に立ち、多数の官民組織のプライバシー関連コンサルタントを行った。共同執筆には、「情報管理体系」(1995年 R.O.メスン、F.M.メスン、セージ)があり、同教授の調査、意見など多数が学術誌、研究書、新聞(ニューヨークタイムス、ワシントンポストなど)で出版、掲載されている。

ピーター・H.デーリー(Peter H. Daly)

米国財務省

行政管理次官補室および最高財務官室相談役

行政管理次官補室および最高財務官室相談役のデーリー氏は、財務レベルでの会計、法律執行、金融システム管理に影響を及ぼす電子マネー政策の問題を専門とする。全米金融サービスボランディア団体の賛同で、1994年にはハンガリー中央銀行で金融改革コンサルタントを務めた。同氏は、ハーバードのジョン F.ケネディ国立スクールでマネジメントクラスの特別講師、上級管理職開発プログラムの相談職員の顔も持つ。委員会では、銀行・財政チームのリーダーを務める。

ジョン C. デイビス(John C. Davis)

国家安全保障局(NSA)

デイビス氏は、NSA の国家コンピュータ安全保障センター(National Computer Security Center)局長を務める。NSA における 34 年間の勤務で、INFOSEC オペレーションズおよび技術サポートグループ副長、調査および技術組織のコンピュータ・公定技術室長など様々なポジションで活躍している。また同氏は米海軍(CINPAC)情報保全部門において、NSA の経理担当最高執行員を兼任する。

トーマス J. フォールヴィ (Thomas J. Falvey)

運輸省(DOT)

情報安全保障事務局長官

フォールヴィ氏は、情報安全保障事務局長を務める。事務局長就任前は、同局内の運輸省の国家安全保障問題担当大統領補佐官であった。同氏は、省内での、輸送や軍事施設の保護と維持、情報戦争、また安全保障に関わる科学技術や研究開発プログラムの専門家である。さらに、化学、生物学、そして核の威力と脅威に関する専門家でもある。物質的安全保障と軍事施設の保護、大量破壊兵器に関する国家安全保障会議の技術支援グループ、および物質流通チームの代表を務める。

ブレントン C. グリーン (Brenton C. Greene)

国防総省(DOD)

国防長官事務局次官・インフラ政策担当次官

グリーン氏は、国防長官事務局次官代表であり、政策担当次官である。委員会に所属する前は、インフラ保障政策とインフラ戦争における政策、計画立案、プログラム手続きを行う国防総省の小グループを率いた。同氏は委員として、エネルギー供給チーム、物質供給チーム、国家エネルギー構造チーム、経済チームなど複数のチームに所属している。

ウィリアム J. ハリス (William J. Harris)

テキサス輸送研究所

ハリス氏は、1997年2月に委員会に参加した、輸送分野の専門家である。同氏は、コンサルティング業務の他、1985年から1995年までテキサス輸送研究所(TTI)の副所長を務めた。同研究所での経験が、インテリジェント道路交通システムの主要プログラムの開発と、長期的視野に基づく輸送問題や、教育、研究と輸送との関係に貢献した。同氏は、バテレ記念研究所で、供給ルート問題、輸送機能停止、第三世界の国々での研究開発、そして国際研究計画の調整に長年携わってきた。また1970年から1985年まではアメリカ鉄道機関の副所長を務め、テキサス輸送研究所の名誉教授となった。委員として、教育認識チームを指導。

デビット A. ジョーンズ(David A. Jones)

エネルギー省安全保障・保護および政策標準分析局長

ジョーンズ氏は、エネルギー省内の安全保障・保護および政策標準分析局出身である。委員会に所属する前は、安全保障・保護のプロの技術組織に所属していた。同組織は、物質、情報、個人的保護、核の制御と責務を含めた規格化手続きと、基本的脅威の形成といったエネルギー省の広範囲に渡る安全保障・保護を開発、公表し、分析する。ジョーンズ氏は、エネルギー委員会のチームリーダーであり、物質流通と研究開発チームのメンバーでもある。

ウィリアム B. ジョイス(William B. Joyce)

中央情報局(CIA)

ジョイス氏は、1972年に中央情報局に入局した。委員会に参加する前は、海外やワシントン州内で、多くの管理職や経営職に就いた。彼の専門は、海外の公的情報の収集および処理と、電気供給システムの開発。ジョイス氏は委員会の権威チームのリーダーである。

ステファン D. ミッチェル(Stevan D. Mitchell)

司法省

ミッチェル氏は、コンピュータ犯罪部門の弁護士である。訴訟を起こし、調査を行い、法案を起草し、高度先端技術の不法使用を管理するために、国際的活動に参加している。委員として、法律の整備チームの責任者となっている。

アーヴィン M. ピクス博士(Irwin M. Pikus)

商務省、輸出管理局

ピクス氏は、委員会に所属する前は輸出管理局に勤務。同局では、米国政府が輸出を管理する高度先端技術に相当する海外の技術に関する情報収集、および分析を指導。同氏の経験は、国家的目標の取組における科学技術の役割に集中している。委員会の、人命サービスチームを率いている。

ジョン R. パワーズ博士(John R. Powers)

連邦緊急管理庁

戦略計画の上級政策顧問

パワーズ氏は、FEMA の上級政策顧問を務める。様々な核兵器対応プログラムの中心的设计者の 1 人。総合的緊急対応能力の政策枠組みの策定、民間セクター内部の動員および防衛に対する方針変更の促進、そして政府機関のための代替紛争解決プログラムの開発を行った。委員としては、国家機構チームのリーダーおよび人命サービスチームの一員である。

ポール・ロジャーズ博士(Paul Rodgers)

法定公益法人協会

ロジャーズ氏は、委員会に加わる以前は、ワシントン D.C. にある法定公益法人協会 (NARUC) の理事および法律顧問を務めた。NARUC には、公益事業および通信事業の規則に従事するすべての州と連邦機関が含まれる。同氏は 1965 年から 1996 年まで、NARUC の理事および法律顧問を務めたが、在職中は議会、行政府および連邦機関内部に認知、尊重される組織として NARUC の役割向上に貢献した。委員会規制チームのリーダー。

スーザン・シーメンス(Susan Simens)

連邦捜査局(FBI)

シーメンス氏はFBIの監督特別捜査官。同局に 18 年間勤務し、コンピュータのスパイ行為プログラム管理を含む国家安全に関する事件を担当。また、同局の対国防総省諜報局渉外担当官も務め、優れた渉外活動により国防総省諜報長官章を受賞。現在、戦略計画分析班 FBIHQ に所属。情報技術問題、装備調達に対する戦略計画に従事し、インフラを脅かす事件でのコンピュータ侵入の裏付けを担当。1973 年から 1979 年まで、米国空軍大佐として勤務。委員としては、人命サービスチームの一員を務める。

フレドリック M. ストラブル博士(Frederick M. Struble)

連邦準備制度理事会

同氏は、重要インフラ防衛に関する大統領委員会金融財政チームおよび経済チームの一員。委員会に加わる以前は、連邦準備制度理事会([Federal Reserve Board](#))に 25 年間勤務。その間、金融機関を監督規制する政策の策定、実行に従事。

ナンシー J. ウォン(Nancy J. Wong)

米パシフィック・ガス・アンド・エレクトリック社(Nancy J. Wong)

ウォン氏は、マグローヒル出版社による「1996 年コンピュータ業界の女性トップ 100」の 1 人に選ばれ、サンフランシスコに基盤をおく米パシフィック・ガス・アンド・エレクトリック社(PG&E)における情報資産およびリスク管理マネージャーという現在の立場から委員会に加わる。同社では、企業の情報技術資産の管理および保護を目的とした開発・実行に携わっている。PG&E の営業範囲は、オレゴン州境界からカリフォルニア州北部のベーカーズフィールドまで 9 万平方マイルに及ぶ。同氏は、国家リスクチームのリーダーを務め、電力供給とエネルギーチームの一員でもある。

参考資料

“Capturing the Importance of Critical Infrastructure Protection”

National Communications System Telecommunications Speech Service, VOL. I, Number 3/17/1998

http://www.ncs.gov/N5_HP/Customr...Affairs/Speech_Service/SS98-001.htm

President Clinton, “Executive Order 13010 - Critical Infrastructure Protection”,

Office of the Press Secretary, The White House, Washington D.C. United States. July 15, 1996

Harry Levins; *Infrastructure Panel taking ‘Cyberthreats Seriously’*; St. Louis Post-Dispatch,

06-19-1977,pp03A. 1997

PCCIP, “Report Summary Critical Foundations”, October 1997

<http://www.info-war.com/pccip/pccip2/summary.html>

PCCIP “Answers to Frequently asked questions”

<http://www.info-sec.com/pccip/web/faq.html>

The White House , Office of the Press Secretary, Annapolis MD, May 22,1998

Fact Sheet Combating Terrorism: PDD62

Fact Sheet Protecting America’s Critical Infrastructures 62

<http://www.info-sec.com/pccip/>

Office of the Press Secretary, “Funding for Domestic Preparedness and Critical Infrastructure Protection”, The White House, January 22, 1999; fact sheet

<http://www.fbi.gov/nipc/fact2/htm>

National Infrastructure Protection Center, “Outreach/Infragard”

<http://www.fbi.gov/nipc/nipc/outreachinfragd.htmact2/htm>

Hunker, Dr. Jeffrey A., “Infrastructure Protection Information Assurance , Congressional Testimony, 06-11-1998

Bridis, Ted,”High-Tech Crime – Fighting Lab Unveiled”,

http://www.infowar.com/mil_c41/99/mil_c41_092599a_j.shtml

Brewin, Bob & Harreld, Heather, ”U.S. sitting duck, DOD panel predicts,” 11/11/96
Information Warfare

Becker, Elizabeth, “Pentagon Sets up New Center for Waging Cyberwarfare”, The New York Times News Service, 08/10/1999

Munro, Neil, “National Journal”, 3/27/99

http://www.infowar.com/mil_c4i/99/mil_c4i_032999c_j.shtml

PCCIP, “Critical Foundations – Protecting America’s Infrastructures,” Chapter 1, page 3, 10/97
http://www.info-war.com/pccip/pccip2/report_index.html

Nancy J. Wong, “The Nation’s Central Nervous System”, PCCIP- Information and Communications Sector Presentations, Briefing to the Advisory Committee, September 5, 1997

<http://www.info-war/pccip/>

Ware, Willis,H., “The Cyber-Posture of the National Information Infrastructure, October 1997, Rand Publications

<http://www.rand.org/publications/MR/MR976/mr976.html>

Reagor, Barbara, “A world with New Rules: How to manage risk in the land of Interconnections and Interfaces. Vol. 102, America’s Network, 02-15-1998, PP S5 (6).

http://www.elibrary.com/getdoc.cgi...143038@library_j&dtype=0~0&dinst=0

Department of Transportation, “Transportation Physical Infrastructure – Description, Goals and policy Framework”, January 1994,

<http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/trd/trd-app.html>

TS&T, “Transportation Infrastructure Assurance”, 1999

<http://scitech.dot.gov/partech/totaltrm/totalterminal.html>

Anderson, Robert H. “Risks to the U.S. Infrastructure from Cyberspace”, Verbal Testimony before the Permanent Subcommittee on Investigations, Government Affairs committee, U.S. S 6/25/96enate

<http://www.cs.edu.virginai.edu/~survive/PAPERS/Anderson.html>

Webv