IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2003 情財第 354 号

電力重要インフラ防護演習に関する調査 報告書

2004 年 8 月

独立行政法人 情報処理推進機構

電力重要インフラ防護演習に関する調査 目次

本調査の背景と Summary

情報通信技術が、金融、エネルギー、交通、医療などの諸所の経済社会活動を支える分野に組み込まれ、社会基盤化してきている現在、悪意ある攻撃によって生じる問題は、事故を引き起こしたシステムやトラブルにみまわた被害者だけの問題ではなく、我が国全体の経済活動の停滞や、国民全体の生命･財産にかかわるリスクをもたらしかねない。

このような状況下においては、情報システムにおける事故や外部からの攻撃が発生した際に、直接の被害や経済社会システムに与える影響を最小化するために、どのような対応をすべきかについて、日頃から検討を進め、体制を整えておくことが重要となる。

本調査では、サイバー事故やサイバーテロに対する演習の実施実績が豊富な米国において実際に行われた電力重要インフラ等に関する演習の実施状況について調査を行い、我が国における重要インフラ等の防護体制について検討した。[1]

なお、本調査においては、重要インフラにおける防護の観点よりその取扱いに関して留意すべき情報が成果に含まれたため、調査報告書の内容および情報源等の一部については、Web 公開の対象としていない。

北米では、「アルカイダなどのテロ集団が電気、ガス、水道などの重要インフラにサイバーテロを仕掛ける準備をしている」との見方を強めている。コンピュータやインターネットという情報時代のテクノロジーを悪用し、経済や国家安全保障が依存されている重要インフラを破壊するという新種のテロの脅威が現出してきている。FBIの国家インフラ保護センター（NIPC）のサイバーテロの定義は「特定地域の住民に混乱と不安要素をもたらす事で恐怖を引き起こすもの」になっている。ＮＩＰＣとは、米国の重要なシステムに対するコンピュータを利用した攻撃を検出、警告、防止する目的を持つ特別組織である。NIPCの初代長官であるMichael Vatis氏が草案を作成し、ＦＢＩ本部に設置した経緯は興味深い。テロリストの心理を分析し、攻撃方法を事前に防止する術を研究しようとする姿勢は、我が国の事後の対処や対策法に主眼を置いている姿勢からは進んでいるように見られる。ＮＩＰＣは、「社会の尊厳を崩す事が、国民的信頼の崩壊に繋がり、社会的不安と混乱を招く根本的な目的である」と、テロリストを分析している。経済の主要なライフラインを破壊する事は、テロリストや攻撃者にとっては、莫大な経済損失を生み出す絶好の機会である。米国の国家安全保障担当官は、「サイバーセキュリティの分野において、ネットワークの障害は国の崩壊に繋がる」と述べている。特に電力網インフラにおいては、都市機能が停止するといっても過言ではない。復旧の長期化により、経済が停止し多くの混乱が発生する。米国は、こうした予測を国家的安全保障や防衛論にまで昇華している。

多くのセキュリティ専門家達が「テロリストは重要インフラへのサイバー攻撃を準備しており、攻撃は時間の問題である。」と語っている。確証の１つは、FBIがアフガニスタンで押収したコンピュータのデータを評価･分析した報告書である。アルカイダが重要インフラに対してサイバー攻撃を準備していることが判明し、これを国家最重要事項と捉えた米国は、現在までに実に多くの「サイバーテロ演習」を開始している。こうした背景を基に、ブッシュ大統領は「国家サイバー防衛戦略プラン」を世界に発表した。

---

[1] 本調査は、独立行政法人情報処理推進機構の事業の一環として、アイ･ディフェンス･ジャパン株式会社（当時。現：株式会社サイバーディフェンス）が実施にあたった。

驚くほどの速さで米国は動き出している。本土防衛安全の為に新省庁DHS（米国土安全保障省）を設立し、17万人を保有する巨大組織も編成した。米軍傘下では多くのサイバー兵士が育成され、民間企業も安全保障部門を新設している。しかも、連邦研究開発（R&D）費の注入で米国経済は活力を増してきた。

我が国も早急に方策や政府の指針を官民連携で実施しなければならない事態にまでなっている。2001年12月27日、オサマ･ビン･ラディンは次のように語っている。「重要なのは、あらゆる手段を使い、アメリカの経済を集中的に攻撃する事だ。アメリカ経済の主要な柱を探せ。敵の主要な柱を攻撃しなければならない」。また、2003年11月16日、アルカイダは「日本人が自らの経済力を破壊し、神の軍勢に踏みにじられたいと思うならイラクに自衛隊を派遣すれば良い。我々の攻撃は東京の心臓部に達するだろう」と述べ、聖戦（ジハード）という意識を固めている。我が国は、テロリストの脅威も抱えており、多角的な対策を望まれなければならない環境にある。

数年前までは、公益事業会社（電力、ガス、下水処理、通信）の多くは、下記のような対処で問題解決が実施されていた。

1）管理システムと運用システムとの分離
2）従業員にモラル教育を行い、注意を促す
3）施設に対する監視の強化
4）データの暗号化

しかし、従業員の経歴や素行を調査するエージェントや分析官は、下記のような方法でテロ攻撃を受ける可能性を導き出している。

1）SCADAシステムに対する侵入
2）ソーシャルエンジニアリングでパスワードを入手し、重要なネットワークに侵入
3）施設やネットワークを物理的に攻撃
4）マイクロ無線回路上のデータを妨害または改ざん
5）内部に潜入した工作員や元従業員など、内部情報提供者を利用した破壊工作

また、実際の稼動システムや制御システムには多くの脆弱性が存在し、危険な状態である事も判明している。このことは、外部コンサルタントの評価や侵入検査の結果を見ても明らかである。米国でのインタビューを下記に列挙する。

○Electric Power Research Institute、KEMA Consulting、Ernst & Young （all involved in cyber security work in the industry）などの専門家は、「以前実施したサイバーテロ演習において、特別チームがコンピュータに侵入して重要インフラの制圧に失敗したことは一度も無い。全てに侵入した」と語る。

○Ernst & Youngとパートナー関係を結んだ前ニューヨーク市市長ジュリアーニ氏が設立した Advanced Security CenterのCraig Crawford氏は、「完全に保護されたネットワークを構築しているクライアントはいなかった」と報告した。

そして、専門家の意見は、「世界中の公益施設は次のような前提で運営されなければならない」と前置きした上で、下記に集約される。

1) 管理制御システムは本質的に安全なものではない
2) 直接的であるかに関わらず、どのシステムもリモートでアクセス可能である
3) 独自のソフトウェアを使用することは危険
4) 制御システムのエンジニア及びオペレータ、ITセキュリティ担当者との間で、システムに関する重要な情報が共有されていない

米国とカナダの電力業界では、最近になってサイバー攻撃に対する防御対策が制定され、それに基づく国家インフラ保護センター（現在では米国土安全保障省の管轄）と電力会社間で自主的プログラムが作成されている。このプログラムは、電力施設等に対するサイバー攻撃と物理的な攻撃の両方に関する情報をリアルタイムに共有することを目的にしている。一般に、他社との熾烈な競争を繰り広げている企業は情報を共有しようとはしないが、エネルギー業界の場合は自由競争の原理にはあてはまらない為、このプログラムが成功していると思われる。

北米のエネルギーISAC（Information Sharing & Analysis Center）は、他の業界のISAC（現在では13以上のISACが存在する）よりも速くインシデント情報を共有することを基本理念に掲げており、エネルギーISACは信頼の高いISACという評判を勝ち得ている。

現在、米国の電力業界が作成しているサイバー攻撃に対する標準対策プログラムでは、参加企業・組織が24時間体制で情報を収集し、安全なwebサーバまたは電子メール、FAX、電話（バックアップのみ）による報告が義務付けられている。

そして、NIPCまたはその任務機関は報告の内容を迅速に分析し、関連性を分析している。警告、警報、アドバイザリを発令するか否かは、諜報機関及び警察当局との協議の上で決定する。特定の企業の機密情報は、一般に開示されないように保護される。

さらに、電力業界のすべてのセグメントから構成される NERC（North American Electric Reliability Council）は、メンバーに対してサイバーセキュリティに対するベンチマークを実施している。NERC は DHS の重要インフラの保護政策においても、電力業界の調整役を行っている。各電力会社の対策が不十分な場合、1 メガワット当たり最大 10 ドルの制裁金が課せられる。

重要インフラにおける制御システムのセキュリティを評価する際、まずはサイバーテロ演習が重要な役割を果たす。1997年に国家安全保障局が極秘に進めた「Eligible Receiver」演習以来、その数は増え続けている。Eligible Receiver演習では、特別チームが重要インフラの制御システムへの侵入に成功したが、これらのシステムはインターネットに接続していない安全なシステムと見られていた。

「Livewire」演習には、多くの業界関係者と政府機関が参加していた。この中には、複数の石油会社やガス会社も含まれていた。この演習に対する参加は任意であったが、参加した企業・組織の名前は今も伏せられている。この演習は従来のものと異なり、単なるテストではなく、米国経済の複数のセクターに対して作戦レベルの攻撃を30日間にシミュレートしていた。Livewireの演習目的は下記である。

1) 各重要インフラの脆弱性の検証
2) 攻撃を受けた企業の対処レベルの把握
    a) 侵入前に検知しているか
    b) 侵入を検知したのはいつか
    c) 対処応報はいつか
3) 政府の対応はどうであったか
4) 今後の長期的な政策課題の策定
5) 作戦、戦術、政策/戦略上の成果収集

演習実施期間中、実際の稼動システムは保護されていた。Livewire演習の運営責任者は「攻撃はwebベースのシミュレーションの範囲内で行われた。実際に稼動しているシステムへの影響は全くなかった」と語った。今後のLiverwire演習は規模も大きくなり、エネルギー業界の多くの企業が参加する予定であるという。この演習の結果、米エネルギー省は米国の国土安全保障戦略に基づく国家インフラに関わる業界が、SCADAネットワークのセキュリティを強化するために準拠する行動規範などを定義した。

米国防総省がサイバーテロの脅威に対する組織を設立したのは 1998 年のことである。しかし、既に 1980 年代の後半にはサイバー脅威に対して関心を寄せている。1990 年代の中頃から国防総省のシステムに対するハッキング件数が年間で数万件を超えるようになったからである。この状況を記録していた米軍は、コンピュータネットワークを防御する専門部隊を設立した。この設立の背景には 2 つの出来事が契機となった。1 つは「Eligible Receiver 97」という軍事演習である。この演習では、擬似的ではあるが、国家安全保障局 (NSA) の職員が軍のコンピュータネットワークに相当なダメージを与えることに成功した。統合参謀本部の本部長が指揮した Eligible Receiver 97 は、軍事および民間の情報インフラへの攻撃に対する防御能力を試すものとしては初めての大規模な演習であった。この演習は予告なしに実施され、電力及び通信会社などの民間のインフラに擬似的な攻撃を仕掛けるだけでなく、国防省や CIA の情報システムに対する「敵国」の攻撃をも想定していた。この演習で行われた攻撃は、高度ではない。脆弱なパスワードやオペレーティングシステムの欠陥を攻撃したり、一般からアクセスできる

web ページから機密情報を盗用したり、あるいはオペレータの研修不足などを利用した攻撃であった。攻撃チームはNSAのスタッフで構成された。このチームは事前に内部情報を全く知らされていなかったが、相当な被害を与えることに成功した。成功要因の 1 つとしては、攻撃対象の機関やサイトに対して事前に電子的な偵察活動を行っていたことが挙げられる。

Eligible Receiver 97 の初期段階では、緊急の電話番号である 9-1-1 を不通にすることも計画されていた。9-1-1 に問題が発生したことを知らせるインターネットメッセージをできるだけ多くの人に送信し、電子メールの受信者に 9-1-1 に電話をかけさせて、この番号を使用不能にするという計画である。これは、実際に不通かどうか確認したくなるという人の心理にヒントを得た作戦であった。

専門部隊を編成する契機となったもう 1 つは、米軍が湾岸戦争の準備を進めていた時に発生したハッキング事件である。このハッキングは当初、イラクの諜報機関の仕業であると思われていた。この事件では、Solaris のよく知られた脆弱性が悪用され、世界各地にある海軍、海兵隊、空軍のコンピュータに対してサービス拒否（DoS）攻撃が実行されていた。この脆弱性に対するパッチ適用は数ヶ月間に渡って行われている。その後、米国政府は史上最大規模の調査を展開し、カリフォルニア州在住の 2 人の若者と首謀者と見られる 10 代のイスラエル人を逮捕している。

2001 年の組織改編で、新たに Joint Task Force Computer Network Operations が組織され、全米情報基盤保護センター（現在は国土安全保障省に統合）、National Communications System（22 の連邦機関と部門から構成される）などの他機関との連携強化も図られている。

現在、米国の民間企業ではタイガーチームを構成することが増えてきた。Cable & Wireless 社では、顧客のインターネットインフラをサイバー攻撃やサイバーテロから守るために、タイガーチームを編成している。民間企業のタイガーチームの場合、法的な背景を持つ多くの実務経験者から構成されることが多いが、事前防御ではなく、事後対応に目的を置いている。つまり、脆弱性を事前にテストするのではなく、セキュリティが侵害されてから迅速に対応する。問題発生後に最初に行われる対策は、顧客のサイトに侵入検知用の機器を設置し、特定のサーバに侵入検知ソフトウェアを導入することにある。

情報保護システムに対する攻撃演習には、最低でも数百万円が必要である。しかし、実際に攻撃を受けた被害額と比較した場合、このコストは必ずしも高額とはいえない。さらには、防護という面でのシステムセキュリティの要件は、擬似攻撃の結果に基づいて設計されるべきである。情報保護の分析には確率的なリスク分析から、幅広い経験に基づくシステム分析まで、様々な方法が必要である。机上シミュレーションだけでは全ての脆弱性を評価することはできない。コンピュータウイルスの世界では、何万というウイルスが認識され、数多くのウイルス検知製品が存在する。非常に多くの労力を割いて 1 製品の 1 バージョンから検知機能をテストしているが、新しい亜種が出現すれば、短時間で広範囲に被害が拡散してしまう。

さらに、それぞれの脅威、攻撃方法、防御方法について、整合性、可用性、アクセス、漏洩、攻撃者の技術レベル、予防、検知、対策で使用状況などの特徴も登録しなければならない。

SAST（Systems Administrator Simulation Trainer）という PNNL のプロトタイプシステムは、不正なアクセスからコンピュータネットワークを保護するためのものではなく、サイバー攻撃からシステムを保護するために何をすべきかをシステム管理者に理解させることを目的にしている。熟練のパイロットであってもフライトシミュレータを使って日常訓練を行うように、システム管理者は SAST を利用して攻撃の検知、侵入者の防止、システムの復旧方法を、毎日学習していく。SAST では、擬似的に攻撃環境を構築し、その環境内でトレーニングツールが自動的に実行される。

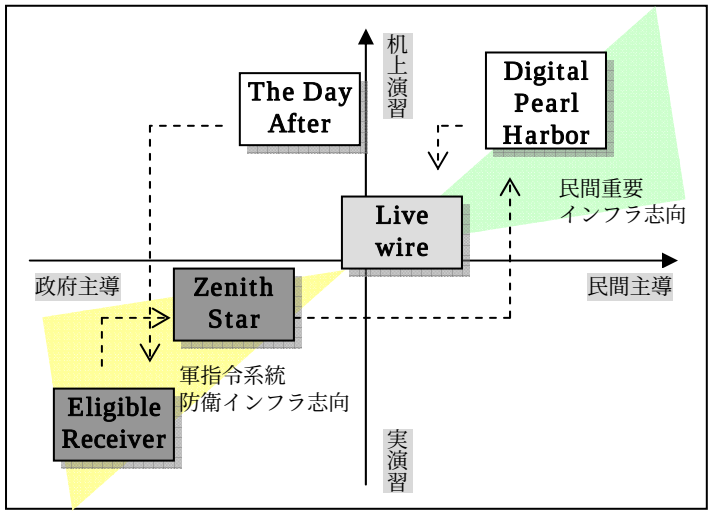
コンサルティング会社の Gartner と米国の海軍大学は、3 日間にわたり Digital Pearl Harbor (DPH)というセミナースタイルの戦争ゲームを開催している。Gartner 社のアナリストと国家安全保障の戦略立案者が、国家の重要なインフラを抱える企業の IT 責任者を集め、サイバーテロ発生時に業界を超えたプロジェクトを遂行するためのシナリオを検討した。このプロジェクトには、重要インフラを所有または管理する Gartner 社のクライアントも参加し、様々なテロを想定して「Digital Pearl Harbor」のシナリオを作成している。しかし、このプロジェクトは机上演習のみであり、システムに対しての実ハッキングは行っていない。セキュリティ担当者が金融サービスや電気通信などの業界別のグループに分かれ、経済、輸送、通信インフラに同時に攻撃を実行して大混乱を引き起こすようなシナリオを作成している。このテロのシナリオの作成には特別な制限は設定されなかった。例えば、Aグループは電力会社向けの IT 管理システムを作成している企業を買収し、その会社のシステムへ自由にアクセスできるようにした上で、米国の主要な 4 つの電力網を攻撃し、中継器を乗っ取り断続的に停電を引き起こすシナリオを計画した。Bグループは、金融機関に対して同時にサービス拒否攻撃を実行するために、世界中にある数千の関連サーバを購入する計画を立てた。また、電気通信分野を担当したグループは、インターネットで売りに出されているカナダのトロール漁船を利用して、米国とヨーロッパを結ぶ海底ケーブルを切断し、6 ヶ月以上通信を不能にする計画を立てた。

2003 年 9 月、Texas-San Antonio 大学の Center for Infrastructure Assurance and Security（CIAS）は、サイバーセキュリティ演習である Dark Screen の最終報告をまとめた。この報告では、机上攻撃と擬似攻撃が含まれている。これは、2001 年 9 月 11 日のテロ攻撃後、最初に実施された大規模なサイバー攻撃演習である。

この様に、サイバーテロに対する防御体制や検知対応能力を強化するために、長い年月が費やされている。このプロジェクトには、非常に多くの都市、郡、地域、連邦機関（FBI を含む）、空軍、民間企業が参加していた。「最新のコンピュータワームと最近東海岸で発生した停電を見れば、情報インフラと電力インフラが決して安全でないことが判る」と Dark Screen 演習の指揮者は述べている。

1. 米国政府機関が実施した重要インフラサイバー防護演習の分析･検討

1.1 米国政府機関の演習実施背景と概括



米国で実施されたサイバー演習は、IT 依存型の軍統合指令系統システムに依存する米軍部が、サイバー戦争勃発時の脆弱性について懸念を抱いたことが始まりであるとも言われている。その背景には、21 世紀のサイバー情報戦争に警鐘を鳴らしている中国軍関係者の名著「超限戦」[1] の影響も大きかった。

サイバー演習の先駆けとなったのは「The Day After」という官民合同の机上演習 [2] であったが、実際の危機意識の基で行われた極秘のサイバー演習という意味では、軍が命令を遂行する上で多くの脆弱性が露見された「Eligible Receiver」が最も有名である。同演習を受けて対策を再検証した「Zenith Star」に至るまで、サイバー演習とは、今で言う重要インフラへの防護演習という側面よりも、米軍部にとって防衛戦略上不可欠な軍事訓練であったと推測される。

次世代のサイバー戦争に備えた防護演習が、民間の重要インフラへの対策も同時に必要だという見解に移行していった背景には、軍部の施設やそれに依存される命令系統システム自体が、かなり民間のインフラと相互依存関係にあることが演習を通して判明したからだと推測される。世界で最も近代的な装備を誇る米軍が過度に IT インフラに依存し、民間インフラと米軍システムの脆弱性が表裏一体である事は、極秘裏に行われた「Eligible Receiver」でも明らかにされている。

米政府や軍主導で行われたサイバー演習は、こうした成果と共に、次に民間セクターの重要インフラへと対象を広げていった。こうした流れと共に演習形態もその様相を変え、実演習から机上演習あるいはインシデント･レスポンス体制の実演習に主眼に変えている。また 9.11 の同時多発テロの影響もあり、脅威の対象を仮想敵対国からテロリストや個人にまで範囲を広げ、一般市民のライフラインを防衛守備する現在のシナリオが形成されていったと考えられる。その代表的な演習が官民協業による机上演習の「Digital Pearl Harbor」であった。

「Digital Pearl Harbor」では完全に民間セクターの視点に立った課題や対策が協議され、かつての「Eligible Receiver」で見られた実演習は行われていない。そのため、演習結果と有用性については専門家の間でも意見が分かれている。

【1】情報セキュリティ総合戦略および iDEFENSE Japan 特別リポートを基に作成

米国サイバー演習の概要 [1]

演習名	実施主体	手法	期間	概要	演習結果
The Day After	DoD	机上	半日	政府や大学など情報インフラ関係者を中心にサイバー攻撃の発生を想定	分散型の適応型のアーキテクチャや早期回復の戦略やシステム構築の必要性がでた。
Eligible Receiver	NSA	模擬攻撃	攻撃 2 週間	米国内の電力システム及び通信会社等の民間インフラへの擬似攻撃を実施。又、国防省やCIAの情報システムに対する「敵国」からの攻撃を想定	軍コンピュータを含む指令系統とその運用インフラである電力系統網に深刻な脆弱性が発見された。
Zenith Star	IATAC	机上	2 日間	Eligible Receiver をベースにした演習で、対応策の改善点を検証	米政府の新組織に必要な双方の情報共有や技術開発を再確認できた。
Digital Pearl Harbor	Gartner, Naval War Collage	セミナー形式	3 日間	国家重要インフラを抱えるIT責任者を招集し、様々なテロ攻撃を想定。業界別に分かれ同時攻撃の可能性を検証	主要な 4 つの電力網を攻撃し中継器を占拠した。継続的な停電を発生させる事に成功した。
Livewire	DHS	机上	5 日間	経済的損失を目的とした攻撃を想定。主要な通信とサービスへの混乱状況を検証し、緊急対応策を検討	各業界セクター間での情報共有体制に問題があった。被害に気付かないケースがあった。広範囲な停電による重要な有線回線が不通になり修復作業に支障が見られた。

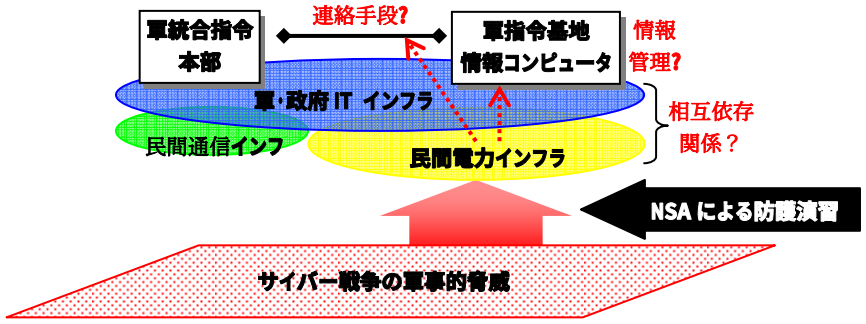
現在、米国のサイバー演習は軍事的側面から民間の重要インフラに対象を移し、同時に学術団体やコンサルティング企業を含めたタイガーチームなどが、民間大手企業のセキュリティ脆弱を対象に仮想演習を行うという市場が形成されている。国土安全保障省も物理テロや生物テロに加えてサイバーテロを混合したシナリオを作成して「Livewire」という演習を行っており、今やテロ演習は米国本土において必要な大規模市場を形成しているといっても過言ではない。

[1] 経済産業省 「情報セキュリティ総合戦略」 2003/10/10 および iDEFENSE Japan 情報局資料を基に作成

1.2 Eligible Receiver

実施期間	1997 年 6 月	目的	中国･韓国地域の 10 万人規模を動員する太平洋軍司令部のグローバル･コンピュータ･ネットワークに対し、情報戦争 (infowar) の模擬演習を極秘に行うのが目的。インフラの脆弱性について検証する。これにより、国防総省のコンピュータの脆弱性および電力インフラとの相互依存性についての危機意識を確認し、他の機関との連携によるインシデント･レスポンス体制を検証。
実施主体	NSA (米国家安全保障局)		
参加者	DoD, JCS, the National Military Command Center (NMCC) in the Pentagon, USPACOM, USSPACECOM, USTRANSCOM, USSOCOM		
攻撃者	NSA の Red-Team 35 人		

全体構図



米統合参謀本部議長の指揮によって 1997 年に実施された Eligible Receivr 97 は、国防総省や全米の重要インフラに対する攻撃を検証する米国の能力テストを課題としてデザインされた極秘演習であり、民間インフラ部分 (電力および通信システム) に対する模擬攻撃も含まれていた。

Red-Team [1] による攻撃の基礎資料は、NSA が特別に手に入れた極秘扱いの情報ではなく、あくまでも公開済みの一般情報や技術ツールがベースであった。内部者による特定情報も与えられず、一般のハッカーや他国の諜報機関が容易に手に入る情報だけで実施していた。そのため、Red-Team は攻撃を開始する 1 ヵ月前からかなりの労力を割いてこの予備調査を行ったとみられ、模擬侵入攻撃はそのわずか2週間後に行われた。

同演習によって、防衛 IT インフラと国家の民間インフラの間では高い相互依存関係にあることが露呈した。例えば、防衛 IT インフラは極端に商用の民間コンピュータおよび通信ネットワークに依存しており、公共･民間セクターはしばしば共通の商用ソフトウェアやシステムを共有している。その結果、国防総省のシステムで露見した脆弱性は他の機関によっても悪用される可能性が否めず、一つの脆弱性が他方面にも影響する事が確認された。

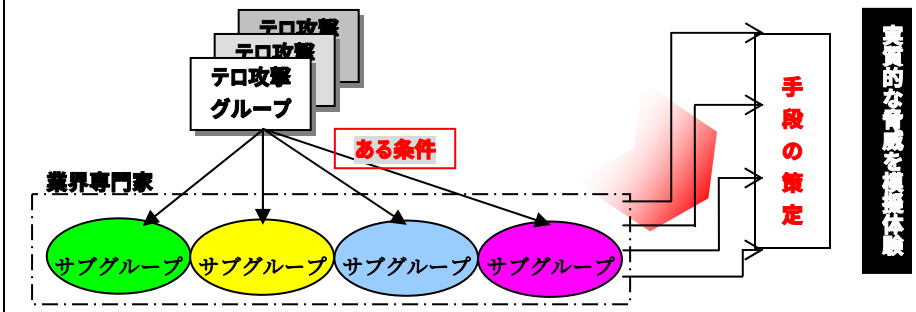
又、システムにおける脆弱性だけでなく、大規模攻撃が発生した場合の対応能力の欠如も明らかになった。貧弱なオペレーションと情報セキュリティ訓練不足が、Red-Team に多くの攻撃機会を与えた。国防総省はこの結果を受けて、政府･軍関連の全てのネットワーク･セグメントに Security Officer を配置し、侵入検知技術も大幅に改善させている。

[1] NSA が演習のために組織したハッカー (攻撃) チーム

1.3 Digital Pearl Harbor

実施期間	2002 年 7 月 （3 日間）	目的	民間セクターで管理する重要インフラを対象にしたサイバーテロの危険性および脆弱性を検証するため、IT 専門家や業界大手の幹部が 3 日間に渡って行った机上演習。基本的な演習プロセスでは、テロリストの視点に立って脆弱性を検証することで、テロの脅威を実際に体感するセミナースタイルの戦争ゲーム方法が取られた。具体的なミッションは、業界セクターの横断組織的な対サイバーテロシナリオの考案。
実施主体	Gartner, Naval War College		
参加者	電力、金融、インターネット、通信関連の専門家や幹部合計 100 社以上		
攻撃対象	民間重要インフラを机上演習		

全体構図



2002 年7月に行った「Digital Pearl Harbor（DPH）」は、3日間にわたるセミナー形式の机上戦争ゲームである。Gartner のアナリストや米海軍大学（NAWC）、セキュリティ戦略者達がロードアイランド州ニューポートに集まり、全米の重要インフラを管理する企業や IT リーダーたちを一堂に会して実施した。机上演習の直接的な目的は、各種業界を超えた包括的な重要インフラへのサイバーテロのシナリオを策定することであった。

しかし、演習の背景には、民間の重要インフラを管理する参加者らにサイバーテロの実質的な脅威を体験させる狙いもあったとみられる。主催者側が参加者を対象に行った事後調査によると、それを裏付けるかのように、DPH ゲーム参加者の 72%は米国を被害対象とする組織的サイバーテロが向こう2年以内に発生する可能性があると回答した。

演習においては DPH 参加者がそれぞれテロリストの役になり、電力系統網、金融サービスシステム、通信、インターネットの4つの重要インフラ分野に対してお互いに協力しながら攻撃するための効果的な戦術を模索した。その目的は、サイバー攻撃によって仮に一時的であれ、戦略的なパワーバランスが移行するような「信頼の危機」を検証している。サイバーテロに対する防御方法が主検証ではない。又、攻撃による被害の経済的損失額などは算定されていない。

Degitital Pearl Harbor の演習の結果、電力系統網に関しては全米規模の停電を引き起こすことは現実的に難しいものの、局地的な被害を発生させる危険性があることは再認識された。この演習結果を踏まえた最終的な提言としては、まずソフトウェアに関するセキュリティや品質自体の改善に加え、

ソーシャルエンジニア攻撃やセキュリティポリシー違反を減少させるための人的レベルの安全対策である。また、オープンソースから得られる情報は比較的浅く断片的なものであるが、一定の専門知識を持つ人間がそれらを収集して攻撃計画することは可能である。次のより深い情報を入手する手がかりレベルの詳細情報を得ることには成功する。従って、できる限りオープンソースの情報を日常的に学ぶことは不可欠である。[1]

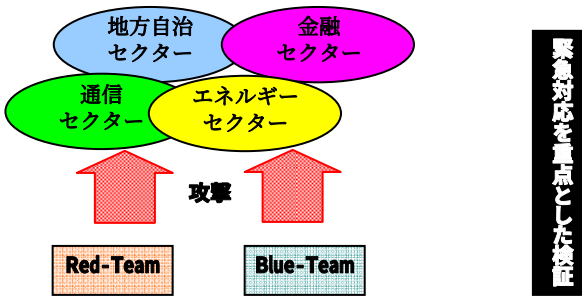
専門家による机上演習の結果、通信や電力インフラなどのクローズドなネットワークに攻撃を行うのは非常に難しいが、一方で攻撃を察知することも極めて難しいことが判明した。逆に金融や IT ネットワークは攻撃が容易である反面、比較的簡単なセキュリティで対策を強化できる。また、対サイバーテロ対策には中央の統制的協力体制が必要であり、政府自体がその役割を担うべきであるという結論に達している。

結論としては、ハッカーがデスクトップの前に座ってリモートから米送電システムを停止させることは非現実的であり、また物理的にも全米規模で停電を引き起こすことは難しい。しかし、限定地域の送電線を停止させることは可能である。又、大きな被害を引き起こすためには、物理的な攻撃および内部不正者の協力も必要となる。SCADA [2] がリモートからアクセスされる危険性もあり、現在のオープン化の流れに拍車がかかれば脅威度も大きくなる。

今後の対応としては、SCADA や送電線のセキュリティ強化に加えて、情報や物理的な施設へのアクセスなどの業界基準を政府が作成するなど、セキュリティの最小ガイドラインやプロセス等の標準を示す必要性が挙げられよう。

[1] "Digital Pearl Harbor and the Grid"　2nd North American Energy Standartds Board ANNUAL MEETING
[2] 重要インフラで一般に導入されている監視制御・データ収集システムの総称　P30 参照

1.4 Livewire

実施期間	2003 年 10 月 （5 日間）	目的	ある程度の被害規模を引き起こす軍事行動レベルのテロを想定。各セクター間や産業別での緊急対応体制を検証し、現行の IR システムとのギャップを特定すると共に課題を抽出して今後の新システムや体制構築プロジェクトのたたき台とする
実施主体	DHS		
参加者	White House, DHS, IAIP, DoD, DoE, DoJ, DoC, DoS, Treasury, CIA, NSA, etc		
攻撃対象	民間の重要インフラを机上演習		
全体構図			

米国土安全保障省が実施した「Livewire」演習は、重要インフラを担う業界側主導で行われた「DPH」に比べてさらに一般市民レベルの脅威や対策を考慮したシナリオをベースにしており、分類的経済損失も想定された。通信とサービスへの混乱状況を検証し、政府と民間セクターによる緊急対応の現状把握と今後の課題抽出を目的としている。

この「Livewire」は、重要インフラへの擬似攻撃や机上攻撃を主眼に置いた過去の演習とは違い、インシデント･レスポンス体制に重点を置いている。攻撃に対する対応策を検証し、National Cyberspace Response System のための分析および課題を抽出している。基本的なコミュニケーション体制や意思決定体制の構築に加え、インターネットを介した組織的かつ戦略的なサイバー攻撃に柔軟に対応するプロセスを検証している。演習後、参加者には管轄管理インフラのサイバーセキュリティ強化の必要性を提示している。

最終的な報告はまだ出されていないが、業界間での情報の流れに問題があったことが明らかになっている。例えば、被害銀行が顧客から口座番号にアクセスできないという苦情を電子メールで送信し、そのときに初めて攻撃されていることを認識するケースもあった。この演習では、米国の重要なコンピュータシステム全体に問題が存在していることも露呈している。

1.5 民間のサイバー演習部隊

タイガーチーム

サイバー演習による擬似攻撃が効果的な手法であると結論付けられた 90 年代末から、民間でも「タイガーチーム」と呼ばれるサイバー演習部隊が急増した。タイガーチームとは、稼動中の防御システムや防御体制能力のテストを行うグループの総称である。海軍基地の防衛能力を試すために海軍が特別な専門部隊を編成するように、このようなテストは間接的に行われることが多い。

元々、米海軍が国防省の通信危機に対処するための部隊をタイガーチームと呼んでいたのが始まりである。近年、米国では政府機関や民間企業に「タイガーチーム」を編成し、危機的状況や緊急プロジェクトなどを迅速に対応している。

例えば Cable & Wireless (C&W) 社では、顧客のインターネットインフラをサイバー攻撃やサイバーテロから守るためにタイガーチームを編成している。C&W 社のタイガーチーム・リーダーは、国際刑事警察機構に招かれ、5 日間の研修と同機構の情報セキュリティの認定コースも担当した専門家であるほか、チームメンバーには元 FBI や NSA なども居る。同チームはセキュリティの脆弱性を検証したい C&W の顧客に対し、侵入検査からインシデント・レスポンス体制までを供給する。

軍部と教育機関の協業

米国 West Point 陸軍士官学校は毎年、米国の他の士官学校とともに CDE (Cyber Defense Exercise) に参加している。この演習は、同校の教官と士官候補生が NSA の資金援助と指導を受けて開始したものである。

CDE は、情報保証 (IA) 課程の上級コンピュータサイエンスの最終課題として位置付けられている。この演習は、同校の士官候補生が設計・開発した CDN (Cyber Defense Network) というネットワークに接続する各地の施設で行われる。これらの施設は、IWAR (Information Warfare Analysis and Research) 研究所が管理している。

.

2. 米国における重要インフラサイバー防護演習結果の分析･検討

2.1 演習後の政府基本指針

米国では、国内外の脅威から守るため、十分に機能する統一的な部署組織を設立するため、第二次世界大戦以来の米国最大規模の国土安全保障省（以下 DHS = Department of Homeland Security）が新設された。従来の政府機関では、生産性が低く非効率的であり、時代遅れな管理や省庁間の連携の不一致などが指摘されていたため、同時多発テロ後、これらの問題を一挙に是正した最終案として DHS 構想を発表している。

DHS に組み入れられた各部門は、元々は 9 つの異なる省庁に属していた。その中でも大きな省庁だった連邦緊急事態管理庁（Federal Emergency Management Agency; FEMA）は、1979 年に設立されている。様々な「救援」「復旧」「緩和」プログラムを持ち、米国各地の緊急事態管理体制を支援してきた。同局は 2001 年、地震･洪水･トルネードを含む 45 件の大規模災害に対処した実績を持つ。FEMA はブッシュ政権から米国内での反テロ活動を主導するという任務を課せられているが、今までは職員数 2,600 人の比較的小さな独立組織であった。[1] それが、2003 年度予算は「情報技術に割り当てられた 1 億 7,560 万ドルを含む 66 億ドルに倍増されている。

サイバーテロ対策部門の新設

DHS のもうひとつの目的は、サイバーテロ対策である。同省はブッシュ米大統領のサイバーセキュリティ戦略案「National Strategy to Secure Cyberspace」及び「Homeland Security Act of 2002」に基づき、「重要インフラの保護」を目的とした NCSD（National Cyber Security Division）を設置した。NCSD は IAIP（Information Analysis and Infrastructure Protection）局の下部組織に位置し、国家サイバーセキュリティ分野に特化している。

この新部門は、サイバースペースにおける政府と民間のセキュリティ分析を 24 時間体制で行い、セキュリティに関する警報を発令する。また、セキュリティ情報の共有方法の改善を定期的に実施し、国家レベルの復旧作業の支援も行う。そのほか、下記の項目[2]についての諸任務を継承し、これらのリソースを最大限に活用して効率的にサイバー情報の資産を運用していく。

- 米国連邦捜査局（FBI）の国家基盤構造保護センター
- 国防総省の国家通信システム
- 商務省の重要インフラ保障局
- 連邦コンピュータ緊急対応センター

また、NCSD の目的は以下の 3 分野に大別される。

---

[1] iDEFENSE 特別リポート「DHS の実態」 2002/12/25
[2] iDEFENSE 特別リポート「国家サイバーセキュリティのための新部門を設立」 2003/7/24

■ 政府及び民間のコンピュータシステムにおけるサイバーセキュリティのリスク評価と脆弱性の改善
■ インターネットで発生するセキュリティ脅威の監視と警鐘のための CSTARC（Cyber Security Tracking, Analysis & Response Center）の運営
■ 他の適切な機関と協力したサイバーセキュリティに関する啓蒙・教育プログラムの開発。及び消費者、一般企業、政府、学術団体、国際コミュニティとのパートナーシップの確立

NCSD は連邦システムのセキュリティに関して、行政管理予算局（OMB）及び国立標準技術研究所（NIST）とも親密に協力し合い、必要に応じて連邦法の執行機関とも協業していく。また、科学技術（Science & Technology）局や財務省秘密検察局（U.S. Secret Service）といった他の DHS 機関も支援する。同部門は情報分析だけに重点を置き、調査収集の機能は担わない。そのため、サイバー脅威に関する情報は FBI、CIA、NSA、その他の諜報機関から入手する予定である。

CWIN

Paul Kurtz 氏は、連邦及び州政府当局によって 2001 年初頭に計画された CWIN（Cyber Warning and Information Network）が全米約 30 ヶ所で既に業務を開始している事を明らかにした。CWIN の発案者は、同時多発テロ直後の 2001 年 10 月、CWIN のような早期警告システムの構築が政府のネットワークセキュリティ対策において最優先事項であると主張した。

情報共有を目論んで構築された CWIN は、既存の National Operations and Intelligence Watch Offices Network をモデルにされている。同ネットワークにおいて国防総省、国家安全保障局、ホワイトハウス、国務省及び CIA の高官は、わずか 15 秒以内に電話で連絡が取れるような体制を敷いている。米経済の様々な産業セクターを網羅する 2 ヶ所の情報共有分析センターはすでにネットワークで結ばれており、2003 年度末にはさらに他の機関との統合も進むであろう。

2.2 民間企業の対策と経済活動

世論の声

「Eligible Receiver」などに代表される軍部主導の秘密裏に行われたサイバー演習は、後に脆弱性と脅威を顕在化させた点では、世論にある衝撃を与えたと思われる。ただし、演習自体が極めて極秘扱いだった背景から、一般市民による不安やパニックといった具体的な社会現象は検証できなかった。

一方、民間主導のサイバー演習は机上攻撃を基にある程度の公開を行っており、結果メディアからの賛否両論も揚がっている。例えば、コンサルティング大手 Gartner などが主催した「Digital Pearl Harbor」は、業界大手による一大イベントだったにもかかわらず、辛口批評が多く見られた。

この DPH 演習に対する懐疑者や批判者の意見を分析すると、幾つかの点が浮かび上がってくる。1つは、「この手の詳細な机上演習を行うことで逆にパンドラの箱を開けてしまい、悪意のあるテロリストに実現可能な攻撃内容を公開してしまった」という指摘である。しかし、同演習前に主催者側が国家セキュリティ担当者と協議した結果、「テロリストは既にシステムの知識を持っており、どのように行動を起こせばいいかも知っている」と想定している。DPH の目的は攻撃者側の頭脳にある攻撃計画を洗い出す点にあり、DPH で使用されたデータやシナリオ情報も、演習以前に知られていたものばかりである。

又、一部の懐疑者達は、「これまでサイバーテロといった事件は起きてこなかった」と主張しているが、世界の一部地域で発生しているコンピュータ障害やワームの拡散などは、テロ組織によるサイバー攻撃テストの踏み台になっている可能性がある。小規模なサイバー戦争の様相も見られている。企業においては、小さいスケールのサイバー攻撃（嫌がらせ。脅迫。犯罪など）が毎日の如く発生している。従って、ほとんどの有識者は DPH の分析が少なくとも有用な参考情報であると認識している筈である。

2.3 9.11 テロ後の国民的危機意識

9 月 11 日のテロで社会的不安と未曾有の恐怖を経験した米国民にとって、「安全」「自己防衛」に対する認識が高まった事は疑いもないが、何よりも変化したのは「国民全体の危機意識」と戦略的に安全防衛案を提案実践しようとする米国政府、そしてその決議を効率よく運用しようとする民間セクターやシンクタンクの団結した意思である。その調和のある連帯感と活動力には、対テロ意識というよりも、戦争に突入した国民の気迫さえ感じる。

9.11 テロの以前から政府関係者の間では、国家の重要インフラとシステムがサイバーテロやサイバー戦争に脆いものだという認識をしていた。国家安全保障電気通信諮問委員会（NSTAC）の主要メンバーは、国家の情報システムの保全が侵入や攻撃の危険に耐ええぬものである事をクリントン大統領に伝達していたが、米国政府自体は情報評価を作成せず先送りしていた。CIA は特に電気通信インフラに対するテロリストの脅威は現実に起こるであろう事を推測し、サイバーセキュリティとサイバーテロに対する問題対処の提案を繰り返しており、早急な情報脅威に関する評価を求めていた。電気通信インフラの攻撃は金融、電力、航空管制といった経済の柱の崩壊も意味していた。実際に 2000 年の「The Electronic Intrusion Threat to National Security and Emergency Preparednes (NS/EP) Internet Communication」では、以下のメッセージが語られている。

「相互接続されたコンピュータへのグローバルなまでの依存と、それがもたらす脆弱性は、サイバーテロを現実的なものとした。テロ集団の向上心は、インターネットを格好の攻撃目標とすることに好都合である。多くのテロ組織は、特定の指導者を持つ階層的な組織から、単一の小組織や準独立形のセル群に変化している。また、特定の指導者がいないが連携し合うグループは、インターネットで連絡体制を構築している。多くのテロ集団がITに興味を持ち、その利用価値を見出している。思想普及や広報活動にもこうしたテクノロジーを利用している。米国の情報インフラの脆弱やサイバーテロ攻撃による潜在的被害も研究している。‥‥‥この問題に対処するには、産業界と政府のかつてない協調と連携が必要である」

クリントン大統領は、秘密裏にサイバー脅威を評価するという事には消極的であったが、政府官僚たちは民間企業との強力なパートナーシップを渇望していた。又、民間セクターの幹部クラスは、既に重要インフラへの脅威データを入手できる構造を許可されていた。重要インフラにおけるあらゆる情報は、企業の死活問題を左右するだけではなく、国民にとっても重要問題であった。

そして、多くのサイバーセキュリティの重要性が議論されている中、同時テロが発生した。アルカイダの攻撃情報を監視しているにもかかわらず、テロは起きている。米国は高度なシステムと最高教育をした人材を投入して監視網を広げている。テロ発生直後、副大統領は大統領オペレーションセンター（PEOC）に避難しており、大統領も別の指揮統制施設に避難している。そして全閣僚を結ぶビデオ会

議がセットされ、ホットラインも各自常設されている。

米国連邦政府では、各閣僚が安全なルートで安全な場所に移動し、政府機能が停止麻痺しないようにしている。最終指揮権限の順位もマニュアル化されている。テロ発生数分後には、国防長官や CIA 長官、FBI 長官、司法長官の大統領国家安全保障チームが召集されテレビ会議が行われる。会議後、各長官が指揮を執るオペレーションも開始される。FBI 本部にある戦略情報オペレーションセンターでは、NIPC が 24 時間体制のサイバー危機活動チーム８Ｃ－CAT が編成される。C-CAT は、物理的な復旧作業支援ばかりではなく、経済インフラを含むその他への追サイバー攻撃に備えて、インターネットインフラを監視する任務も背負っている。

NIPC は、緊急時の対策と情報共有を迅速に対処した組織である。特殊技術アプリケーション部隊を連携させ、大量のデータを格納、分析していく。

又、ＦＢＩと共同で幾つかの情報共有分析センター（ISAC）を設立、指導している。現在 NIPC は、重要インフラに関する物理的な脅威情報を収集し、それを発電所や電気通信施設、水道会社、金融機関といった重要インフラを所有及び運用する数千の民間企業に渡す作業を始めている。こうした情報共有活動は様々なＩＳＡＣ設立として拡大している。

テロ発生時点で、すでに金融サービスや電力業界、電気通信業界、情報技術業界、コンピュータソフトウェアのアンチウイルス業界で ISAC は確立されていたが、NIPC は最近さらに多くの ISAC を立ち上げている。現在、米国民の共通した意識は「正確な情報」「迅速な情報」「適切な対処」に向けられている。国民は、こうした警告、発令を連邦、州に期待している。

これに対し、ブッシュ大統領は、国民に向けて下記の「最終サイバーセキュリティ戦略の概要」を発表した。

1）警戒・緊急情報ネットワークを導入する
2）国土安全保障省が連邦政府及び業界の一括情報報告窓口になる
3）政府機関でサイバー攻撃の影響を評価する訓練を行う
4）商務省が IPv6 関連のセキュリティ上の問題を検討する
5）国土安全保障省が IPS に「コード規範（code of good conduct）」の適用を提言する
6）エネルギー省及びその他の関係機関は、SCADA といった分散コントロールシステムの安全性を確保するベストプラクティスを策定する

さらに、政府、企業、及びコンピュータユーザーが考慮すべき点として、5 つの優先重要事項を提示した。

1) セキュリティ応答システムのセットアップ
2) 脅威及び脆弱性の特定
3) 認識の向上とトレーニング
4) 主要な政府系 web サイトの安全性の確保
5) 国内外の協力の促進

しかし、この発表ですぐさま反応を示したのは民間企業である。DHS の新設と新国家サイバーセキュリティ戦略によって、政府から何十億ドルもの新規受注を受けられる可能性が出てきたからである。これら企業の多くは、冷戦の終了とインターネットバブルの崩壊という二重の景気後退に悩まされていた。

2002 年には、「対テロ資金」に約 300 億ドルが連邦政府から捻出され、多くの金額がサイバーセキュリティ関連に充てられていた。SRA の最高業務責任者 Ted Legasey 氏は、「米国家防衛の構想を最も広義に解釈すると、今後数年間で 1,000 億ドルもの金が準備されるであろう」と推測した。

今後、米国国家安全保障においては、これまで以上に大きな役割を民間企業が任されると思われる。RAND 社が最近創設したシンクタンクのディレクターを務める Randy Larsen 米空軍大佐は、「民間企業は、単に爆弾や銃弾を提供するだけでなく、作戦上重要な情報分析などの任務もこなすであろう。」と語っている。民間企業を取引対象としている政府機関のリストは、Directory of Homeland Security という新しい要覧にまとめられており、500 以上の米国連邦、州政府機関の連絡先と米国家防衛予算の詳細が列記されている。

こうした国家安全保障商品の経済的活動が高まる一方で、米国市民の関心は反テロ法案の1つであるパトリオット（PATRIOT）法に向けられている。アメリカ自由人権協会（American Civil Liberties Union）は、国民の心情を代弁し、「新法は、我々が安全かつ自由に生きることのできる憲法による保護を根本的に覆す・・・・」とコメントしている。

この法案は、米国司法省が起草した。法執行権限を政府に供与する法律の改編案であり、2003 年1月に完成された。120 頁もの膨大な量に渡り、条項には初の国内暗号化規制も盛り込まれている。この法案は、リベラルな米国人から猛烈な批判を引き起こし、国会においても未だ論議の的である。この「非合法な暗号使用」についての法案が可決されれば、連邦犯罪を犯す可能性がある者（有罪の証拠となるあらゆる通信を隠蔽するため、意図的かつ故意に暗号化技術を使用する容疑者又は疑わしい者）に対し、懲役刑が科せられる。インターネット使用の一環として日常的に暗号化を行っている多くの専門家は、この法律を非難している。また、司法省は 1 回の裁判所命令だけで、容疑者の web に対応した携帯電話の音声・インターネット通信を監視し、デバイスのメモリ内容を入手できるようになる。これにより、逮捕令状なしの逮捕が公認され、死刑が増え、DNA データベースが増大すると考えられている。

従来よりも広範囲の電子捜査･盗聴権限が供与され、国家が攻撃された場合、大統領は関与したと思われる人物の米国領土内における全財産を没収する。

この新法の主な条項を下記に抜粋する。

1）第 201 項「テロ捜査の拘束者に関する情報開示の禁止
（Prohibition of Disclosure of Terrorism Investigation Detainee Information）」
情報公開法により、政府が拘束したテロ容疑者に関する資料の発表を拒否する司法省の権限を強化する。

2）第 301 項から第 306 項「テロリスト識別データベース（Terrorist Identification Database）」
テロ組織の疑いのある組織と関係のある人物、何らかの犯罪の容疑がかけられているか、テロ組織と称される組織を支援している非市民を含む「テロ容疑者」に関する DNA データベースの構築を公認する。
･･･これは、反戦活動に署名しただけの人間もデータベース登録される事を意味する。

3） 第 312 項「法執行機関による捜査活動に関する適切な対策
（Appropriate Remedies with Respect to Law Enforcement Surveillance Activities）」
2001 年 9 月 11 日以前の州裁判所による全判決のうち、人種差別、市民権の侵害に無関係であるものを破棄する。それにより法執行機関による個人及び組織の情報の収集を制限し、今後の差し止め命令に何らかの制約を課す。

.

3. その他の国における重要インフラサイバー防護対策

3.1 カナダの場合

現在、カナダのサイバーセキュリティ界は、明確な要素で構成されている。重要なインフラには、物理的なテクノロジー設備及び情報テクノロジー設備、ネットワーク、資産などがあり、これらが崩壊すると、カナダ国民の健康、安全、セキュリティまたは経済の健全性、カナダ政府の機能に深刻な影響を及ぼすと位置付けられている。

カナダのセクターは、国内の投資家間の議論や国際的な情報交換によって識別されている。

- 通信及び情報テクノロジー（電気通信、ソフトウェア、ハードウェア、ネットワーク（インターネット））
- エネルギー及びユーティリティ（電力、天然ガス、石油生産、輸送システム）
- 金融（銀行、セキュリティ、投資）
- 食品（食の安全性、農業及び食品産業、食品流通）
- 政府（政府機関、政府のサービス（例えば、気象情報サービスなど）、重要な国の象徴（文化施設、遺跡、記念物など））
- 保健医療（病院、研究所、薬局など）
- 製造業（化学工業、防衛用兵器の生産、防衛産業基盤）
- 安全（化学、生物、放射性物質、原子力安全性、危険物、救急サービス（警察、消防、救急隊など））
- 輸送（航空、鉄道、船舶、陸上輸送）
- 水道（飲料水、排水管理）

サイバー対策活動は、情報テクノロジーシステム及び資産の発掘と復元に焦点が当てられている。これには電気通信、コンピュータ及びソフトウェア、インターネット、衛星、コンピュータ及びネットワークの内部接続、また、これらによるサービスの提供などが含まれる。

また、攻撃対策として政策やプログラムが配備または開発されており、重要なサービスを迅速に復元できるようになっている。カナダ政府は脆弱性などの脅威を特定し、重要なインフラの所有者や管理者に警告及び指示を行うことを目標にしている。

信頼性のあるリーダーシップを図るために、カナダ政府は最初に国の重要なインフラを所有する者に対して適切な保護対策を、物理的な範囲やサイバースペースにおいて確約している。これには、緊急事態の対応計画、政府のシステム・手段・資産に対する継続的な計画が必要であることが表明されている。

2001 年の 9.11 のテロ事件以降、カナダ政府は、州、地域及び民間セクターと協同してプログラムを推進している。この大きな目的は、政府と民間セクターとが協力して、より発展的で回復力の高いインフラを形成することである。また、協力することで相互に情報を交換することができ、より直接的に調査及び開発を行う。さらには、危険性、脆弱性、脅威に対する対策や相互依存性を発展させることができ、今後の NCI 活動に貢献することも可能にしている。

特定のセクターでは、脆弱性、脅威、侵入及び異常に関する重要な情報を一元管理しており、情報の共有や分析を行うことに価値を置いている。現在のような環境では、政府の活動だけでは、極めて重要なサービスを確実に保護することはできない。一元的な情報共有の概念は非常に重要であり、カナダ政府は、このような情報共有体制の開発方法に関して各機関と連携して検討を行っている。

また、カナダ政府は政府高官による部門間委員会を設立した。ここで検討される事項は、影響を受ける部分もしくは影響を受ける重要インフラが予測できず、対応策や被害を軽減する方法が明らかでなく、国内外のどこで発生するかも明確でない状況を想定している。

民間組織は国家インフラの多くを有しており、サイバースペースの保護で重大な役割を担っている。Canadian Electricity Association（CEA）、Canadian Bankers Association（CBA）、Canadian Telecommunications Emergency Preparedness Association（CTEPA）などの組織とカナダ政府の情報共有の拡充が現在のテーマである。

民間組織は、サイバー事件が犯罪または国家安全に対する脅威の疑いがある場合、カナダ連邦警察（RCMP）またはカナダ公安情報局（CSIS）に直接連絡する。報告者側で事件の種類を判断することが難しい場合は、Government Emergency Operations Co-ordination Center に報告され、CICS（Cyber Incident Coordination System）Cyber Triage Unit で検証される。この部署は OCIPEP、RCMP、CSIS の職員がメンバーとなり、事件を判断して適切な初動及びその後の措置を決定している。CICS は、サイバー事件と脆弱性に対応する総合的且つ組織的な統合システムを提供している。

3.2 英国の場合

英国で「The Troubles」と呼ばれる北アイルランドとの抗争が 1960 年代後半から激化し、1998 年の Good Friday Agreement が調印されるまで続いた。この抗争での死者は 3,000 人にも上り、その大半は一般市民であった。英国本土が最初に攻撃を受けたのは 1939 年であり、このときコベントリとロンドンで爆破事件が起きている。英国の支配下にあった北アイルランドの統合を求めるアイルランド共和国軍がテロ活動を本格的に開始したのは 1950 年代初頭である。

以上の歴史的背景から、米国と異なり、第 2 次世界大戦中も敵国による空爆の脅威に晒されていた英国では、自国の無防備さに対する国民の自衛意識が高い。9 月 11 日に米国で発生した同時多発テロ以降、英国では 500 人以上がテロ対策法に基づいて逮捕されているが、有罪が確定した者は殆ど居ない。それでも英国のテロ対策は世界で最も厳しい法律であると言われており、テロリストに有益な情報を所有していたと見なされただけで逮捕される。。

英国国民は、テロの脅威に対してとても高い関心を持っている。2004 年 3 月 4 日に発行された Associated Press-Ipsos によると、66%がテロの脅威を懸念しており、その中の 21%が非常に心配であると答えている。それに対して、米国ではテロの脅威を懸念していると回答したのは 63%であった。

英国のテロ対策法は2000年に改定され、国際的なテロ活動に対処するための枠組みも制定された。この法では、犯罪者の引渡しに関する権限が改正され、被疑者の国籍に関わらず、テロ活動に関与した容疑者を他国の法廷でも裁くことができる。この法律は、2003年のExtradition Actでさらに強化された。

Immigration and Asylum Act 2002の第4条「the Nationality」では、以前に他国の国籍を取得していた者又は二重国籍者には、英国の市民権を認めないことが定められた。英国のDavid Blunkett大臣は、犯罪立証の基準を、現在の「合理的に疑いの余地がない」から「非常に可能性の高い」に変えることを提案した。ロンドンのキングズ・カレッジのInternational Centre for Security Analysisのセンター長であるBill Durodie氏によると、同大臣は予防処置として自爆テロの可能性のある人物を逮捕できるように法整備を行うべきとの考えを示したという。

Newton of Braintree 上院議員が議長を務める Privy Counselor Review Committee は、2003 年 12 月に提出した報告書の中で、英国のテロ対策法に関する批判を展開している。この報告書は議会でも取り上げられ、少数政党である自由民主党の McNally 卿は「反テロ活動において英国政府は隠れ家に後退すべきではない」とテロ対策法を擁護した。

英国では9.11の同時多発テロ後まもなく、Anti-Terrorism Crime and Security Act of 2001が制定され、

テロ活動の捜査に必要と見られた場合、電話会社及びインターネットサービスプロバイダに通信記録の保存を強制することが可能となった。しかし、政府関連機関はテロ対策に関係がない場合でも、利用者の詳細、請求データ、電子メールのログ、携帯電話の発信元などに関する情報を入手できる状態にあり、このようなデータの保存と利用に関する障害を排除するために、論理的な法的枠組みが求められていた。英国政府は、データの保存義務をテロ対策という特殊法案ではなく、基本的な法案の中で扱うべきかどうか検討している。

また、Regulation of Investigatory Powers Actなどへの組み込みも検討されているが、通信技術の急激な発展が反対に障害となっている。これは、新技術の出現に伴って保存対象のデータ、保存期間、開示要求の条件などを随時速やかに改定しなければならないからである。これまでは傍受した通信記録を証拠として採用することが禁止されていたが、これを緩和すべきかどうかも議論されている。このような緩和は新たな犯罪に対処するために必要という意見もあるが、その妥当性については現在検討中である。

テロ活動を事前に検知し、未然に防ぐために通信データの最低保存期間を設定すべきかどうかも議論中である。ヨーロッパでは、基本法案の中で最長期間を制定している国も存在しているが、大半の国々は英国に歩調をあわせ、2次法案の中で保存期間を設定している。

英国政府が近々発行するWhite Paper on Organized Crimeの中では、組織的な犯罪だけでなく、テロ活動にも対処できるように法を改定すべきかどうかの議論も取り上げられている。2001年9月11日から2004年1月31日までに、英国のTerrorism Act 2000に基づいて544人が逮捕されている。この中で98人がTerrorism Act違反で起訴されている（下記の資料を参照）。ただし、この数字は英国、スコットランド及びウェールズのみのものであり、北アイルランドでの逮捕者は含まれていない。

Individuals charged under the Terrorism Act 2000

According to police records, the 98 individuals charged under the Terrorism Act were charged for the following 155 offences:

Number of offences	Specific offence	Relevant part of the Act
59	●Possessing an article in circumstances which give rise to a reasonable suspicion that his possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism	s57(1)
28	●Belonging or professing to belong to a proscribed organisation	s11
12	●Collecting or making a record of information of a kind likely to be usesul to a person committing or preparing an act of terrorism ●Possessing a document or record containing information of that kind	s58(1a &1b)
7	●Receiving money or other property intending that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism	s15(2)
6	●Entering into or becoming concerned in an arrangement which facilitates the retention	s18

	or control by or on behalf of another person of terrorist property	
6	Failing to disclose information as soon as reasonably practicable that may be of material assistance ●in preventing the commission by another person of an act of terrorism ●in securing the apprehension, prosecution or conviction of another person, in the United Kingdom, for an offence involving the commission, preparation or instigation of an act of terrorism	s38(b)
6	●Receiving instruction in the making or use of firearms, explosives or chemical, biological or nuclear weapons	s54(2)
4	●Receiving instruction in the making or use of firearms, explosives or chemical, biological or nuclear weapons	s54(2)
3	●Providing instruction or training in the making or use of firearms, explosives or chemical, biological or nuclear weapons	s54(1)
3	●Providing instruction or training in the making or use of firearms, explosives or chemical, biological or nuclear weapons	s54(1)
2	●Wilfully failing to comply with a duty imposed under or by virtue of this schedule (Port and Border Controls)	Schedule 7 Para 18(1)
2	●Possessing money or other property intending that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism	s16(2)
2	●Entering into or becoming concerned in an arrangement as a result of which money or other property is made available or is to be made available to another, and 'he' knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism	s17
2	●Interfering with material which is likely to be relevant to the [terrorist] investigation	s39(2)(b)
2	●Belonging or professing to belong to a proscribed organisation	s11
2	Failing to disclose information as soon as reasonably practicable that may be of material assistance ●in preventing the commission by another person of an act of terrorism ●in securing the apprehension, prosecution or conviction of another person, in the United Kingdom, for an offence involving the commission, preparation or instigation of an act of terrorism	s38(b)
2	●Possessing an article in circumstances which give rise to a reasonable suspicion that his possession is for a purpose connected with the commission, preparation or instigation of an act of terrorism	s57(1)
2	●Collecting or making a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism ●Possessing a document or record containing information of that kind	s58(1a & 1b)
1	A person shall be guilty if he does anything outside the UK as an act of terrorism or for the purposes of terrorism and his action would have constituted the commission of one of the following offences if it had been done in the UK: ●Sec 2,3 or 5 of the Explovise Substances Act 1883 (causing explosions, etc.) ●Sec 1 of the Biological Weapons Act 1974 (biological weapons) ●Sec 2 of the Chemical Weapons Act 1996 (chemical weapons)	s62(1)
1	●An offence under section 2, 3 or 5 of the Explosive Substances Act 1883 (causing explosions, etc.)	s62(2)(a)
1	Possessing an article in such circumstances as to constitute an offence under ●The Explosive Substances Act 1883 ●The Protection of the Person and Property Act (Northern Ireland) Act 1969 ●The Firearms (Northern Ireland) Order 1981	s77(1)
1	Receiving money or other property intending that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism	s15(2)
1	Entering into or becoming concerned in an arrangement as a result of which money or	s17

other property is made available or is to be made available to another, and 'he' knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism

4. 米国電力会社におけるサイバー防護演習事例の分析・検討

4.1 自由化が進む米電力会社の運用現状

1990年代の相次ぐ法律制定が起因となって、電力業界の規制は大幅に緩和された。それに伴い電力業界でも構造変化が起こり、制御システムを内部および外部に公開するなど、サイバー空間の脆弱性が新たな問題となっている。

規制緩和以前の電力企業は、縦割り式に統合された地域の独占企業であり、保証利益率を維持するために州当局が価格を調整していた。エネルギービジネスの全ての課題を決定していたのは、各地域の独占企業であった。それが規制緩和後、これまでの独占企業は発電、送電、配電、集金および顧客サービスなどの各部門別に分割され、各市場それぞれに対して新規参入が可能となった。

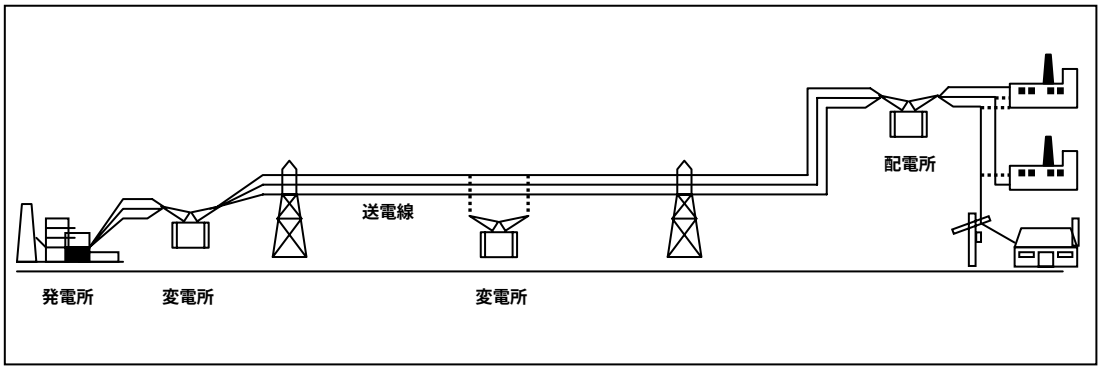
電力は一般市場で購入することが義務付けられ、必要な運転予備電力はこれまでの20～30%から10～15%に低下した。また、自動制御システムが、発電、送電、配電用に利用されるようになった。

ところが市場の統廃合と柔軟なエネルギー取引によって、脆弱性が生まれてしまった。コスト削減のために知識や経験豊富な従業員が解雇されて重要情報の漏洩につながる一方、残った従業員は人的リソースが低下する中でさらなる責任を負っていく。比例して、制御システム運営者が現場に不在の場合や、そういったシステムへの遠隔通信手段を利用する場合が増え、システムへのリモートアクセスの頻度が高まった。また、自由化されたエネルギー取引の効率化のために、制御系システムと業務系ネットワーク間の相互接続も進んだ。その他、規制緩和と新規ビジネスの拡大によるM&A（合併買収）の普及で、異なる組織や会社の旧来の技術仕様を接続統合する必要が生じ、これにより情報の安全性の点から新たな脆弱性が生まれた。

SCADA（Supervisory Control and Data Acquisition）システムは米国の重要インフラ（電力、ガス施、通信など）において過去30年間使われてきた。ところが過去数年間で技術革新が進んだインターネット技術の普及で、リモート接続によるリアルタイムのデータ通信が可能になった。これを可能にしたのが、XMLのデータ形式やSQLデータベース、ブラウザを使ったウェブ表示等のオープン技術である。このオープン技術が、結果的に脆弱の穴を露呈させ、攻撃の対象にされる頻度を高めてしまった。

4.2 米電力会社のシステム環境

米国内の電力網は非常に高度な相互接続で動的に構成されている。その構成組織は、公共・民間施設、地域の共同組合、商事会社など 3200 以上の組織であり、その下位構成として地域単位の電力網が存在する。電力業界はさらに、発電、送信、供給、顧客サービスなどの各システムに区分されており、それ以外に電力の売買システムがある。「現代のエネルギーシステムの目標とは、できるだけ信頼性のある経済的で安全な方法で電力を発生させ、それを顧客に供給することである。と同時に、重要な稼動レベル（電圧、周波数、位相角）を許容範囲内で維持することである」。



SCADA システムが提供する3つの主要機能は下記である。

●SCADA サーバからのデータ取り込みおよび、同サーバへの管理コマンドの送信
●監視カメラを含むリモート機器からのデータ取り込みおよび、同機器への管理コマンドの送信
●迅速な意思決定を行うための集合データへのアクセス供給

4.3 技術的な脆弱性の問題

米国では深刻化する通常のサイバー脅威に加え、特に重要インフラを管理する制御システムへのサイバー攻撃の危険性が増大している。ここでは重要インフラの防衛と制御システムのセキュリティ対策を取り上げる。

脅威の要因としては以下の理由が考えられる。
1）共通の標準技術への移行による脆弱性
2）制御システムと他システムとの相互接続環境の問題
3）制御システムにおける最新セキュリティ技術の導入限界

1）の共通の脆弱性とは、Windows や UNIX、オープン製品などの標準技術を指す。これまで独自のハードウェア、ソフトウェア、通信プロトコルを使っていたプロプライエタリな制御システムは、外部から運用方法が見えにくかったためにハッキングされる心配が少なかった。しかし、現在は競争優位の点から低コストで高機能性を追及するため格安の標準技術に移行しており、通信手段もインターネットで利用されている標準プロトコルを採用。これらの技術には周知の脆弱性が存在し、簡単に利用可能で効果的な攻撃ツールも広範に出回っている。それを狙った攻撃方法が、現在増えている。

特にデファクト・スタンダードで世界第 1 位を占める米国 Microsoft 社の OS は、反米感情が加速する中で最も攻撃対象に選ばれやすい。攻撃側にとっても Windows の情報は入手しやすく、広範に普及していることから被害効果も高く狙いやすい。世界標準化は今や、それ自体が深刻な脅威になっている。

2）におけるネットワーク化の問題も、ニーズが先行してセキュリティ対応が後手に回っている。システム間同士やパートナーとのネットワーク接続によって、リアルタイムの情報通信や管理、モニタリングなど多くの利便性を享受できる一方、インターネットという廉価な広域通信網に存在する深刻な脆弱性が標的にされている。

3）の限界とは、最新セキュリティ技術の導入、パッチの適用、ユーザー認証の強化といった一般的な安全対策が役に立っていない現状を指す。これは制御システムが元々、サイバーセキュリティを想定して構築されていないことに起因する。

例えば、権限の許可／認証技術、暗号化、侵入検知、通信／トラフィック・フィルタリングなどの最新セキュリティ技術は、より多くの帯域やプロセッシング・パワー、メモリなどのリソースを消費する。しかし、重要インフラの各ステーションでは通常、システムが特別な処理を迅速に行うようデザイン構築されているため、リソース抑制の観点からプロセッサ能力をできるだけ抑えている場合が多い。運用に支障を来たさず、最新のセキュリティ技術を導入することが難しいのである。

また、電力企業がシステムに採用しているメインフレームそのものも問題視されている。米セキュリティ政策を考える民間団体の Vanguard Technology Alliance によると、これまでのインフラ保護対策はインターネットとコンピュータシステムを中心に実施されており、最も重要な要素であるメインフレームが無視されている。これらのメインフレームシステムに対する偵察行為や攻撃行為は逐次報告されており、政府機関、軍施設、大手企業などの重要なアプリケーションやデータがサイバー攻撃の危機に直面している。次のターゲットとしては、民間セクターで大型汎用機を導入している大手のインフラ企業に向けられる可能性が極めて高い。

同団体は、メインフレームのセキュリティが 5 年前に比べてかなり脆弱になっていると指摘する。メインフレームにおける管理やセキュリティは確かに向上したが、メインフレーム自体のセキュリティ・レベルが後退しているという分析である。更に、メインフレーム向けのセキュリティ対策資源が減少しており、セキュリティの脆弱に歯止めがかかっていない。同団体は政府に提出した最近の報告書の中で、メインフレームのセキュリティ基準が除外されている点を厳しく非難している。

4.4 対応策

仮に強固なファイアウォールや認証方法を導入して制御システムを隔離しても、アプリケーションや運用レベルにおける必要な R&D（調査開発）が不足していることが問題である。実際のセキュリティ技術と、制御システムを防御するのに必要なインテリジェンスの間には、常にギャップが存在しているとする指摘もある。

広範なセキュリティ分野を網羅する R&D の強化によって、制御システムを防御するためのより効果的な技術開発や対策が期待されている。R&D が投入される分野には、例えば異なる制御システムアプリケーションで必要とされるセキュリティ技術の特定、許容パフォーマンスの基準設定、侵入検知システムにおける攻撃パターンの解析、インテリジェンス情報などが挙げられる。

潜在的な脅威に対処するためには、全般的に以下の点が挙げられる。[1]

・制御システムを防御するための新しいセキュリティ技術に向けた R&D の強化
・制御システムに特化したセキュリティポリシー、ガイダンス、標準化の策定。例えば、強力なセキュリティ投資を促すための技術標準やコンセンサスの推進
・強固なアーキテクチャやセキュリティ技術を導入し、セキュリティの意識改革と情報（インテリジェンス）の共有。例えば、強固なファイアウォールや認証方法を導入してコントロール・ネットワークを隔離し、より安全なネットワーク・アーキテクチャを構築する。また、幹部クラスによるサイバーセキュリティ・リスクの教育や実施プランによって、企業全体のセキュリティ意識を向上させる
・制御システムを含む効果的なマネジメント・プログラムの導入。これらのプログラムには通常、リスク・アセスメント、適切なポリシーや処理手順の開発、従業員の意識改革、常時のセキュリティ監視などが含まれる
・緊急障害発生時におけるオペレーションの安全性と継続性の確保に向けた、企業内での各種セキュリティ・プランの開発と試験。継続的なオペレーション・プランの推進

継続的オペレーション・プラン例

- 業務遂行における重要度のアセスメントとサポート・リソースの特定
- 業務の早期回復と潜在的被害の最小化
- 包括的な継続プランの開発とその明文化
- 継続プランの定期的な試験と適切な修正

最後に、政府と民間が協力してセキュリティポリシーやガイドライン、業界基準などの開発を行い、セキュリティに向けた意識改革と情報共有体制の確立などを議論すべきである。例えば、米政府は民間

[1] iDEFENSE Japan 特別リポート ID#031101 「米国におけるサイバー攻撃の脅威」

と協力して業界標準を策定し、双方でコミュニケーションが図れるための Information Sharing and Analysis Center（ISAC）を確立している。

安全規則や勧告による対策

電力インフラの保護は、米国の中でも最重要課題となっている。「業界全体の基準や市場の考え方は常に反作用をともなう」という声もあるが、大規模攻撃の発生前に電力業界における有効な安全手順と対策を実施する場があることは確かである。連邦エネルギー規制委員会（FERC）の関係者は、エネルギー施設の運営者やその他の専門家と話し合いを持ち、電力市場に参加する全ての組織を対象にした義務的な安全規則を作り上げている。

2004年1月1日に施行されたFERC規則は、物理的および電子的な安全性を守るための最低限の保護対策を「運用中の監視インフラ、緊急対応手順、および商用ソフトウェアとシステム」に規定している。また、エネルギー省エネルギー保証局による脆弱性調査や、同局が作成した安全性ガイドラインによって、それに続く勧告も促された。一連の勧告は追加項目の過程を経て補足され、制御システムの安全性に要求される特定の課題を反映するように改善される。

同様に重要なのが、脆弱性と脅威についての最新情報を絶えず入手し続けることである。ITの脆弱性と脅威に関する情報は現在、エネルギーISAC（現在情報共有分析センター）[1]を中心に共有されている。制御システムの電子的な脆弱性と侵入被害の正式検知や、その情報が共有された事実は今のところないが、制御システムの電子的な脆弱性やその被害に関する情報を収集するセンターを全ての業界で設立することは、それが規定の全ISACにとっての情報源になるという意味で重要なことである。

電力制御システムの安全性を確保するために、以下の重要勧告を考慮する必要がある。

- □ 全てのリモートアクセスポイントを含む「安全性の境界線」を確定し、境界線内の重要な物理的および電子的施設を保護する。これには人・物・通信の出入り口がすべて含まれるべきである。また、アクセス管理の条件は明記される必要がある。
- □ 管理ネットワークへのリモート接続を最小限に抑えて安全性を高める。具体的には、接続は絶対に必要な制御システムへのリモート接続のみにとどめる。監視、管理機能、維持管理を目的としたネットワークの使用は可能とするが、その他の全てのリモート接続は禁止にすべきである。また、システム運用が要求されるリモート接続では通信を暗号化し、強力な認証方法を使用する必要がある。
- □ 企業の業務系ネットワークと制御システムの接続をできるだけ最小限に抑え、安全性を高める。現在、業務系ネットワークと運営制御システム間には非常に多くの回線がある。その回線についてはほとんど把握されておらず、無視されているか無防備となっている。不必要な接続は遮断し、残り

[1] http://www.energyisac.com/

の回線はファイアウォールや侵入探知システムなどの安全対策ツールを使用して安全性を高めるべきである。業務系ネットワークと制御システム間の接続は商業活動に不可欠だが、複数の分離した回線を使用するのではなく、全ての回線が通過する個所に十分に保護された接続ポイントを配置した方が良い。

□ また、定期的にソフトウェアの欠陥にパッチを当て、ウイルス対策ツールなども利用する。企業の業務系システムが適切に保護されていれば、関連する業務系ネットワークを経由した制御システムへの間接的な攻撃リスクを低減させることができる。

□ 制御システムと関連する業務系システムにおいて、可能な範囲で強力な認証とアクセス制御を実装する。現在、双方のシステムにおける認証とアクセス制御は十分とはいえない。デジタル署名やセキュリティトークン、そして生体認証を利用して、制御系ネットワーク経由の接続を対象に認証を行い、アクセス権の運営と管理を厳格に行うことが必要である。

.

5. ヒアリング結果を基にした脆弱性調査の分析･検討

5.1 サイバーテロの現実的な脅威

コンピュータスキルを持ったユーザーの世界的増加と共に、ハッキングツールはネットを介して広範に広まり洗練されてきた。ハッカーは簡単にツールをダウンロードし、クリック1つで攻撃を開始する。攻撃コードは短期間に開発され、脆弱箇所を自動スキャニングするツールと抱き合わせた複合手法でコンピュータを素早く乗っ取る。被害に遭ったコンピュータは、次のターゲットを狙うために新たな加害者となる可能性がある。

脅威の分類

脅威	解説
犯罪グループ	不正利益を狙ったグループ単位でのサイバー侵入が増加している
外国諜報機関	諜報活動やスパイ活動の一環として、外国諜報機関あるいは諜報サービスによるサイバーツールの使用が報告されている
ハッカー	愉快犯によるリモートからのネットワーク侵入に加え、サイトでの攻撃コードの交換などによって簡単な手段で広範囲を攻撃する手口が横行
ハックティビスト	行動が政治的に動機付けされているサイバー活動家で、サイトやメールサーバを攻撃して政治的メッセージを送る活動を展開する
情報戦争	複数の国は情報戦争に積極的に関与しており、ドクトリンやプログラムの開発、技術習得などに奔走している。情報戦争は軍隊能力だけでなく製造･通信･経済などに深刻な打撃を与えることが可能
インシデント脅威	企業に不満を持つ内部者や委託先ベンダーの関係者などによるコンピュータ犯罪が考えられる。この場合、犯罪者は内部アクセスが可能なため、特別なハッキング技術を必要としない
ウイルス･ライター	ウイルス･ライターによる脅威は感染力の強さと共に増加傾向にある

制御システムに関する一般情報は、ハッカーや侵入者にとって簡単に手に入れることが可能である。例えば、電力施設に関する製品データや技術者向けの教育ビデオなどの一般情報は、電気工学の初歩を学ぶために利用される。一方、FERC (連邦エネルギー規制委員会) の資料や産業公開情報、工業地図、その他の関連書類などはすべてインターネットから入手できるため、ハッカーはこれらの情報を基に最も利用されている送電ラインやノード施設、重要な発電基地の場所を推測する。

また、制御システム自体に関するデザインや管理資料、相互接続の技術標準、RTU や通信機器間の基準といった情報も一般入手が可能である。情報ソースはその他にもある。元従業員、提携先ベンダー、アウトソーシング (委託先) 事業者などに加え、同様のシステムを利用する他の施設のユーザー情報などである。つまり、入手先には豊富に存在する。ハッカーはこれらの情報を的確に分析し、システムを習熟して的確な攻撃方法を模索していく。

制御システムに対するサイバー脅威は、今や米政府や専門家の間では緊急課題となっている。過去において管理者が下していた決定事項も、現在ではシステムが一部自動機能となっているため、サイバー攻撃による推定被害は以前にも増して甚大である。

テロを仕掛けるのは、敵対政府からのテロリスト集団、不満を持つ従業員、犯罪組織、そして個人ハッカーまで多岐にわたる。諜報機関やテロリスト集団などの十分な攻撃リソースを抱える組織にとって、攻撃対象に足を踏み入れずに、その国の重要施設に体系的かつ大規模なサイバーテロを行うことは決してバーチャルな空論ではない。

敵国家

20ヶ国以上がサイバー戦争用の戦力を積極的に発展させていると考えられる。その数は非対称紛争の時代を背景に増加する可能性が高い。該当する国家は、最も深刻な脅威を与えるに足りる資源や技術、そして運営制御システムに関する知識を有している。

サイバーテロリスト

この言葉の厳密な定義に従えば、今日に至るまで一般的に知られたサイバーテロリズムの事例はない。しかし、テロリストグループは間違いなくIT技術を磨いてテロに応用している。現時点ではその技術を使用して通信の機密化を図り、新たなメンバーを採用し、想定される攻撃対象（電力施設やエネルギー運営制御システムを含む）の情報を収集し、宣伝活動を行っている。米政府関係者はテロリストグループがサイバー攻撃の技術を発展させていると考えており、ハイテク化したテロリストが信念や目的を共にする敵国家に支援されている可能性があるとしている。

ハッカー

ハッカーの身元は多くの謎に包まれている。ティーンのハッカーや幼稚なクラッカー（スクリプトキディー）の大多数は、その技術や専門知識が深刻な障害を与えることはないと思われている。本当の脅威を及ぼすのは、エネルギーシステムとネットワークに関する詳細な知識を備え、ネットワークへの侵入と不正アクセスの経験を持つ技術に長けた少数のハッカーグループである。テロリストグループや敵国家の有給サービスで働く専門のエリートハッカーは、運営制御システムを混乱させる危険性が高い。環境団体の一員、もしくは反資本主義者でもある政治意識の高い少数のハッカーが、重要インフラを妨げる動機と技術を持つ場合も脅威となる。

内部者

会社に反抗心を持つ社員や元従業員が、制御システムの専門知識を利用して、重要インフラシステムの円滑な働きを脅かす恐れがある。しかし、同様のEMSやSCADA技術は世界中で使用されているため、運営制御システムの「内部」知識は広く入手可能である。

過去の重要インフラ被害事例

過去数年、全国の重要インフラを監視･管理する制御システムにおいて、多くの事件が発生している。2000 年春、製造ソフトウェアを開発した豪企業の元従業員が地方公務員職を断られた際、無線送信機を使って同地域の汚水処理施設の制御システムに侵入し、264,000 ガロンもの未処理下水を近くの河川や公園に放流した。

また、2003 年 1 月、マイクロソフトの SQL サーバを狙った Slammer が、VPN 接続を介してオハイオ州 Davis-Besse 原子力発電所の個人コンピュータネットワークに感染し、SCADA システムを約 5 時間にわたって停止させた。同施設のプロセス･コンピュータも停止し、再運用までに約 6 時間を費やしたほか、他の電力施設を結ぶ通信トラフィックも混乱し、通信の遅延や遮断に追い込まれた。

96 年には弱冠 19 歳のスウェーデン人が自宅から米フロリダ州南部の電話ネットワークシステムに侵入し、同州内の 12 ヶ所から自動リピート電話による緊急電話 911 番への DDoS 攻撃を行った事件が報告されている。物理攻撃の直後にこのようなサイバー攻撃が発生した場合、緊急対応が混乱することは容易に想像できる。

NSA（国家安全保障局）によると、複数の外国政府はすでにコンピュータへの攻撃能力を備えており、米国を仮想敵とする政府は米システムの技術知識や攻撃方法などについて深く研究している。NIPC の 02 年1月の報告書によると、オサマ･ビン･ラディン氏と間接的につながりのあった個人のパソコンには、ダムまたは給水施設の構造技術に関するプログラムが見つかっている。また、一部の米政府機関や諜報機関は、アルカイダのメンバーが給水および浄水施設を管理する制御システムの情報を、多くの Web サイトから入手していた形跡があると発表している。

米東海岸大停電とテロ疑惑

アルカイダテロリストグループは公式声明において、2003 年 8 月 14 日に北米を襲った大規模な停電を引き起こしたと主張している。声明の中で、今回の作戦は「オサマ･ビン･ラディンの命令に基づいて米国経済の柱を攻撃した」ものであり、問題の方法については公表していないが、「神の兵士がこれらの都市の電力を切断した」と述べている。

カナダの Canadian Office of Infrastructure Protection (OCIPEP)による 2001 年 11 月の報告では、「米国の法執行機関及び諜報機関は、アルカイダのメンバーが SCADA の情報を探しているという兆候を発見した」ものの、主に水道（衛生）システムに関するものだったという。また、アルカイダは重要なインフラに関心を移しつつあるが、「アルカイダが重要なインフラに対するサイバー攻撃を仕掛けた例はない」と語っている。

最も影響を受けた公益事業会社の FirstEnergy 社が、データが送電網の障害が発生する数時間前か

ら「中西部送電網における電圧の異常変動などの異常な状態」を示していたことから、GE 製 XA/21 システムのバグが原因だとする最終報告が出されている。

米国の電力網には脆弱性があるものの、そのハッキングに成功して同規模の損害を与えるには、非常に精巧な技術と忍耐を要し、真剣かつ複雑な組織的作戦で行われなければならない。新たな証拠が出ない限り、アルカイダの主張の信憑性は低いが、アルカイダが米 SCADA システムに対して関心を寄せている点は間違いない。これは実際に進行中の脅威として捉えるべきであろう。

一方で、大規模停電の 3 日前から猛威を振るった Blaster ワームが SCADA システムに関する通信手段の遅延の原因に挙がっている。直接的なサイバーテロの可能性は不明瞭だとしても、これらのワームを使った間接的なサイバー攻撃は、政府のシミュレーションでもすでに証明されている。

又、2001 年 4 月 25 日から翌 5 月 11 月にかけて、米カリフォルニア州全域の送電を制御するコンピュータシステムがハッカーからの攻撃を受けている事実も判明している。同ハッカーはカリフォルニア州 Santa Clara とオクラホマ州 Tulsa のインターネット・サーバを使用して Solaris 製 web サーバ 2 基の脆弱性を攻撃して侵入に成功したが、技術の未熟さからシステム全体を乗っ取ることができずに発見されていた。

5.2 攻撃方法の検討

2002 年 7 月の NIPC（国家インフラ保護センター）の報告によると、サイバーと物理的な攻撃を融合した「swarming attack」の可能性が、重要インフラにとって新たな脅威となっている。サイバー攻撃を物理攻撃と同時あるいはその直後に行うことで、被害側の対応の遅延や混乱をいっそう誘発させる効果がある。例えば、電力システムを不能にするサイバー攻撃を物理攻撃と合同で行うことで、緊急時の行動規範や電力供給などの対応を混乱させる戦術が考えられる。米国では重要インフラの代替施設や代替運営等の対応はできず、ほとんどの修理部品等も国外から取り寄せているため、被害の復旧にはかなり時間がかかるものと予想される。

イラク開戦に反痰するアルカイダ新派「Melhacker」による米国攻撃用の Scezda ワームや、東南アジアの政府サイトを狙った Yaha ワームなど、侵入したシステムにネットワーク攻撃型の不正プログラム（ウイルスやワーム等）をばら撒いて帯域超過による停止を引き起こす。トロイの木馬を組み込んだ攻撃手法も存在する。

間接的な攻撃手法として、テロリストなどによる物理的な攻撃の準備段階で IT 技術がかなり多用されていることが確認されている。アルカイダは新たな自爆テロ候補者の募集を IRC（インターネット・リレーチャット）で行っているほか、グループのプロパガンダ普及にアングラサイトを活用している。また、9.11 のテロリストグループがイメージファイルに暗号やメッセージをエンコードする技術を活用して極秘通信していた事実もある。その他、最近社会問題化しているスパムメールにおいても、例えば CyberSad's Gang や 0102、X-Teg などのハッカーグループはスパムメールに細工を施しす方法で極秘通信に利用している。

5.3 マイクロ波攻撃

電力系統を事故などから保護するシステムとしては、マイクロ波によるマイクロキャリアリレーシステムがある。これは落電事故などがあっても事故区間を迅速に切り替えるよう無線（マイクロ波）で制御信号等の通信を可能にしている。広範囲な地域に敷設された巨大かつ複雑なシステムである電力設備を監視･制御し、運用するには、自らの判断と責任によって管理が出来る高信頼の通信回線が必要である。このため、電気事業では、この通信回線を通信事業者の回線によらずに、自社で構築し維持管理している。

マイクロ波に関しては、米国、中国、ロシアが軍事的目的で開発を進めているが、テロリストによって攻撃手段に変わる可能性もある。

5.4 対応策

ニューメキシコ州カートランド空軍基地の空軍研究所は、E爆弾戦争における攻撃と防衛の研究に取り組んでいる。ソ連軍が 1940 年代には既に E 爆弾の実験を始めていたと言う報告もある。実際、ロシア議会の議員が次の様に語っている。「本気でアメリカを痛めつけたいのであれば、原子爆弾を米国上空で爆発させて電磁パルスを発生させ、米国全土の送電線網、コンピュータ、衛星を含む通信インフラを破壊する。」

2001 年には、英国の防衛産業企業である Matra Bae Dynamics 社が、無線周波を利用して敵のエレクトロニクス機器を破壊する実践用 E 爆弾を開発した事を発表した。

E 爆弾は核爆弾よりもはるかに製造が簡単であり、高価なミサイルを投下せずに戦闘機の回路を破壊できる兵器である。1998 年には、米国海軍の元電気技師である David Schriner 氏が自宅の地下室で 500 ドル足らずのパーツで E 爆弾を完成させた事を米国議会に報告した。この話を聞いた議会は、その後 Schriner 氏と巨額の契約を結んだ。一方、電磁パルスの脅威を研究する調査委員会の任命を Donald Rumsfeld 国務長官に命じている。

米国がネバダ砂漠で行った初期のテストでは、テスト地から 150 キロメートル先のサーキットブレーカが落ちた。しかし科学的研究の優先順位は、核爆発の爆風及び熱影響の分析のみに絞られていた。記録データには、一つの電磁波 4 5 ポンド以下で数ナノ秒以内に 1 ギガワットのパワーを放出するとある。アメリカのフーバーダムが一日に生成する電力が 2 ギガワットであるとすれば、この恐ろしい脅威が容易に想像できよう。

EMP は、広範囲に広がる危険な静電気である。「静電気」のパルスは、他に類を見ないほど高強度の電磁波で運ばれる。核爆弾の爆発により瞬時に真下の大気全体が巨大な無線送信機、すなわち最高の周波数を放射するアンテナとなる。そして核爆発からのガンマ放射の影響は、高度約 40 から 50 キロメートルの大気を伝わり地表の大部分にまで及ぶ。

地球磁場によって急速に拡大した稲妻（fireball）によりコンプトン電子効果が高まり、結果としてマイナスの電子がプラスの原子核から分離する。この分離により、電子が地球の磁力線に沿って螺旋状に下降し大量のエネルギーが生成され、電気系統や電話といった長距離金属線に被害を与える。そして、コンピュータや携帯電話、航空通信、自動車の電子制御点火装置といった装置、システムに被害を与える。

被害は落雷の何千倍もの速度で広がるため、ほとんどの種類の避雷装置は基本的には役に立たない。また、エネルギーは光速で伝わるため、EMP は爆発地点から四方八方にほぼ同時に到達する。1

回の爆発だけでこのようなパルスが日本、あるいは北米大陸を覆ってしまう。このような兵器の殆どが核爆発で生成される。

長い間、西側諸国の一般市民及び主流の科学学界は、2 つの理由から EMP がもたらす被害を認識していなかった。理由の 1 つは、こうした実験が太平洋中部の島やネバダ砂漠のように遠い所で実施され気付かなかったことである。2 つ目は、当時の社会がコンピュータの基本部品であるトランジスタ、マイクロプロセッサに現在ほど依存していなかったためである。

専門家によって公開された報告書によれば、過去 EMP の防衛費は、軍事システム経費の 10 パーセントを占めていたが、現在ペンタゴンでは対 EMP 防衛計画に多くの時間と経費を費やしている。1 人の科学専門家は、過去 30 年間に対 EMP 防衛及び影響に対する調査分析費として、米国防衛原子力局（U.S.Defense Nuclear Agency）では毎年数億ドルが支出されていたと推計した。

多くの専門家は、米国軍で対策が講じられていても、実際に EMP の爆発実験が起きた場合、高確率で多くの通信にダメージを与えるであろうと警告している。もちろん、その他の国々における被害状況も同じである。北朝鮮やパキスタン、イスラエルの反政府分子、ハイテク能力を持つテロ組織から電子爆弾が発射される可能性は高い。小型の EMP 爆弾を利用すれば、容易に先進国の経済活動を不能にできる。EMP は低コストで巨大な脅威を与えられる兵器である。大気圏で爆発しても直接的には米国市民を殺傷しないが、米国の通信及び IT インフラを一掃し大混乱にさせる事は容易である。大気圏層及び周波数帯への対策は早急に国家レベルで行うべきであろう。

アルカイダといったテロ組織が、原子爆弾を検知する権限を持つ米エネルギー省の NEST チームの超厳戒態勢を潜り抜けて、小型 RF 爆弾に方を製造している可能性もある。核兵器ではない EMP 爆弾ならば容易に隠蔽する事が可能である。

6. 電力重要インフラの脅威及び脆弱性に関連する情報の分析・検討

6.1 8.14 米東海岸大停電の現状

2003 年 8 月 14 日、木曜日、16：15 頃発生した停電は規模としては 61800MW（東電の最大需要に逼迫する）。約 5000 万人に影響を与えた。初動原因は錯綜しているが、オハイオ州の発電所脱落後、送電線が過負荷で遮断したことが第一にあげられる。

悪化した原因としては、

1）クリーブランド地域南部の送電線の連鎖的遮断。
2）潮流の迂回による不測事態を監視するリレーシステムの対応不良。
3）正確な情報収集の遅延による現場の判断ミス。
4）系統運用者のヒューマンエラー。
などが指摘されている。

又、分析した専門家は下記の関連要因を挙げている。これは我が国においても参考になる項目である。

1）系統運用の複雑化
2）運転員の対応遅延
3)内陸立地などの地理的条件の調査不足
4）系統構成の複雑化。多岐に渡る管理会社の連絡網未整備。
5）事故波及び防止設備の未完全
6）流通設備の投資不足、老朽化の未リフォーム
7)広域送電線の煩雑計画増加
8）運用者の権限不足

特に、広大な北米東北部の電力系統は地理的、歴史的に電力系統の構成が複雑になっており、競争激化と電力自由化に伴う電力設備会社のコスト（システムが老朽化しても修復コストが掛かり困難、人材教育が悪化、現場の権限が小さい⇒責任者レベルまでの連絡遅延）の問題が相乗的に足を引っ張り合っていた。

結果、トラブル発生から停電⇒都市機能麻痺⇒2 次的被害の拡大、悪化⇒復旧、沈静まで、企業活動への影響を含めた経済損失は 1 兆～3 兆ドルといわれており、未だ算出不能となっている。

再停電の発生や損害を最小限度に抑える為、一部地域の計画停電などを行いながら、全面復旧計

画を進めていた。

送電線のトラブルを発生させたニューヨークの Con Edison 社（以下Ｃｏ.）や負荷喪失が発生し発電所が停止した LIPA 及び NYISO は、それぞれ原因や情報収集と把握、毀損状況の点検などに奔走していたが、市民への情報提供も随時行っていた。

NERC（北米電力安定供給協議会）や連邦政府、州、市の各行政も独自レベルの情報収集をマスコミ報道や各プレスリリースなどの情報を資料としながら対応の整理を迅速に行っていた。

配慮した主な事項は、
1）テロとの関係
2）復旧時期
3）都市機能麻痺による生命の安全確保
4）過去のデータに基づく治安確保の手順
5）都市機能停止の回復状況

である。特に猛暑の時期でもあり「飲料水の確保と飲水の奨励」は頻繁に行われていた。

45 分以内でＦＢＩはテロの可能性を排除し、DHS は「州及び地方自治体、エネルギー部門と協力し、必要な対策への対応と原因究明にあたっている」と声明を出している。17 時 50 分には政府高官による緊急電話会議がセットされ、「テロリストが電力網の脆弱点を探っていた」事実などが話されたが、結局ブッシュ大統領は 20:00 頃「テロのいかなる証拠もない」という声明で国民の不安を鎮めている。

この間 14 日には、エネルギー省のキール・マックスロー副長官は連邦エネルギー規制委員会（FERC）、連邦緊急対応庁（FEMA）、原子力規制委員会（NRC）、国土安全保障省（DHS）、北米電力安定供給協議会（NERC）などの電力関係組織を召集し、調査を開始している。さらに 15 日にはカナダとの共同調査委員会の共同議長をエネルギー省長官が国際的なチーム団を発足した。

州では緊急対応計画が進められ、パタキ州知事が州都オールバニーの緊急対応指令部に退避し、ニューヨーク州緊急事態宣言を州民へ発動した。さらに、州兵、州警察、州関係当局員を動員し、ＮＹ州公共サービス委員会、ＮＹ州独立系運用と電力会社との連携を誘導し緊急電力の確保に動いている。

ニューヨーク市は対テロ緊急対応計画「アトラス計画」[1]を発動し、緊急司令部を設立すると同時に「停電対応計画」も開始した。米国においては、連邦や州、市が独立した機能を持つ事は認知であるが、個々の緊急チームの重複作業や有り方は参考になる。我が国における、縦割り行政の管轄において

[1] ニューヨーク州の対テロ緊急対応計画で、人的な専門チームの配備と交通システムの保安からなる。

も重複する事項が存在する。これらを十分に整理し緊急対応することが望まれる。

6.2 大停電の分析結果からみる脆弱性

停電が発生した直接的事象と拡大した要因は公表されているが、インターネットへの意図的な攻撃及びサイバーテロの可能性は否定されている。しかし、アルカイダが電力網を調査していたという事実やシステムがウイルスに罹っていたという報道が徐々に公表されるに至っては、偶然にも自然的災害、人的ミスが頻発したとは云いきれない。又、原子力プラントが被害拡大の要因にならなかった事は幸運であったが、発生した場所が北米の大都市であり、消費量の高い真夏であった事が国民的不安を増大させている。

従って停電の原因となったシステム的脆弱性のみを分析するのではなく、都市機能麻痺という2次的被害及び社会的影響も分析していきたい。

今回の大きな被害要因は、警報システムの故障と重なるバックアップの不調、さらには運転員の認識遅延と事故対応能力の未熟など「システムとヒューマンエラー双方の不運」である。

原因の1つにシステムのバグがあった事は、最近判明している。ゼネラルエレクトリック（以下GE）社のエネルギー制御システムに欠陥が指摘されている。下記はニュースになった記事である。

> FE[1]によると、停電から数週間後、GE社とある請負業者が管理するGE社のXA/21システムの集中コード監査にバグが発見されたという。「現段階ではまだ確証があるわけではない。この問題は非常に細部に存在しており、何万というコードとデータの分析には数週間が必要」と広報担当のRalph DiNicola氏は述べている。アメリカとカナダの合同調査委員会による2003年11月の報告では、この欠陥が原因で、FEの制御センターにあるAkronの警報システムに障害が発生したという。調査報告では、この欠陥が事前に判明していればFEによる事前対応も可能であり、停電の拡大を防ぐことが可能であったと語っている。「警報器や画面上のアラート、アラームログからシステム状態の僅かな変化を読み取り、電力システムを制御しているが、FEではこのような警報装置が作動不能であった。さらにFEでは警報無作動を認知していなかったため、システム上で問題発生を感知できなかった」と分析されている。結果、連鎖的に発生した障害により、アメリカ合衆国の8つの州とカナダで電力の供給が絶たれた。（以上）

また、Blasterワームがインターネット上で猛威を振るう最中に発生したため、Blasterと停電の関連性も推測されている。2003年初めにFEが管理する電力発電所の2つのシステムがSlammerワームの攻撃を受けたというSecurityFocusの報告もあったため、この推測は高いと見られている。しかし、FE側によると、XA/21のバグは、監視装置で発生した不審なイベントとアラーム状態によって発覚したという。サーバのバックアップにも失敗し、メインシステムに障害が発生してから未処理のプロセスの実行も不可能であった。FEでは電力供給網の状態を出力情報で監視していたが、システム障害は1時

[1] FirstEnergy社の略。停電前に同社の重要なコンピュータが障害を起こしており、被害のきっかけとなった。

間以上にわたって気付かなかったと報告されている。

報告書では、高圧の送電線に倒れた木を FE が撤去しなかったことも問題にされている。NERC では、停電の再発防止策が各電力会社に勧告された。その一つには、FE による XA/21 システムのパッチインストールも含まれている。FE は、GE 社が修正をリリースした 2003 年秋にバグに対するパッチを適用したという。また、XA/21 に代わるシステムへの切り替えも実施している最中だという。しかし、この切り替えは停電発生前から計画されていた。

北米電力網の構造を検証してみると、電力グリッド（送電網）は、大きく分けて Western Interconnection（米西海岸）、Eastern Interconnection（米中部及び東海岸）、ERCOT Interconnection（テキサス州）の 3 つの部分に分割されているのが判る。電力は保存できず、ガスや水道のようにバルブを開閉して提供するといった管理もできないため、必要に応じて発電し、AC（交流電気）では物理の法則に沿ってネットワーク内の送電線を自由に流れていく仕組みになっている。

又、複雑な送電網を管理して快適な電力を標準供給するために、NERC（10 団体の地方組織がメンバー）が 7 つの利用項目に基づいて運用標準を策定している。この NERC は 1965 年に発生した大規模停電の教訓を経て 1968 年に非営利団体として創設されている。8.14 の大停電の際は、10 団体のうち ECAR、MAAC、NPCC の 3 団体が影響を受けた。これらの 10 団体の地域をさらに細分化すると、北米で 140 ヵ所のコントロールエリアに分かれる。各エリアの送電センターには高度のモニタ・コントロールシステムがあり、年間 365 日 24 時間体制で監視している。以前は電力会社が発電、送電、販売の 3 部門を垂直統合で保有し、この各エリアを運営管轄として業務を展開していたが、最近の自由化に伴う規制緩和によってそれらを分離した ISO や RTO などが登場してきた。ISO や RTO は独自の送電施設を持たず、複数のコントロールエリアにまたがってメンバー会社の資産を管理・運営して電力卸売市場を管轄する役目を果たす。8.14 の際は、5 つの RTO/ISO が影響を受けた。ISO や RTO は複数のエリアを総括してサービス提供および緊急危機管理地域の範囲としている。これらの地理的範囲は、北米で 18 地域ある。

原子力発電所への影響

直接的原因はなかったものの、全米 9 ヵ所の原発が緊急停止（リアクターが停止）。また、カナダでは 7 ヵ所の原発が緊急停止したほか、別の原発が過度電流のため自動的に電力系統から切り離された。そのほか、米 6 基およびカナダ 1 基は深刻な電力被害を被ったが発電を続行している。

SCADA システム

8 月 14 日の大停電により、電力業界で広く使用されている SCADA システムに対するリモートアクセスが議論の的になっている。2003 年 8 月 14 日の Computerworld.com には SCADA システムの脆弱性に関する記事が掲載された。この記事では、電力会社はより正確な統計情報を記録し、電力の販売を

拡充するために、電力の供給状況とフローをリアルタイムに監視するコンピュータを社内の LAN に接続しているが、その結果、SCADA システムが脆弱になったと指摘されている。

電力の供給状況を監視する PC ベースのソフトウェアはファイアウォールによって保護されているが、リアルタイムの制御系装置にはこのような保護対策はされていない。制御システムに対してもファイアウォール、侵入検知、暗号化や認証機能を構築する重要性が強調されているが、大停電の発生までに議会において電力業界のサイバーセキュリティの強化と制御システムの保護に必要な予算を審議する動きは見られなかった。

8 月 14 日の大停電の影響を分析する上で他の要因も考慮する必要はあるものの、Windows ベースの LAN から SCADA システムにリモートから接続していたことと、それによる脆弱性が存在していたという事実は重大な要因のひとつとして指摘されている。

<u>このような状況を招いた背景</u>

電力業界が一夜にしてこのような問題を抱えたわけではない。これは規制緩和とともに始まっている。電力業界ではコスト削減と合併の動きが強まり、各企業はコスト削減の方法を模索していた。その 1 つの方法として、これまでの専用システムに代わり、一般に普及しているオペレーティングシステム (通常は Microsoft OS) が採用されるようになった。しかし、本質的なことを考えると、専用システムを使用している方が安全性は高い。

また、Blaster ワームが電力会社や他のデータ通信ネットワークに与えた影響について重要な点は、ネットワーク上の 1 つの Windows システムが当該ワームに感染しただけで、Windows ベースかどうかに関係なく、ネットワーク上の全てのシステムやコンピュータのパフォーマンスに影響を及ぼす点である。

大停電は非常に短時間で拡大した。多くの報告によると、9 秒以内に停電が発生していることがわかっている。発生までの時間を見る限り、不正なプログラムによるネットワーク障害は、自体を悪化させただけで、大停電自体は別の要因によって発生した可能性も考えられるため、大停電の原因と不正プログラムの関係については、より詳しい分析を行う必要がある。今後、電力供給の安全性と信頼性を維持するためには、電力業界が現在抱えるサイバー攻撃の脅威をなくすために、政府と電力会社が協力して問題を解決していくことが最も重要である。

6.3 大停電後の米国政府機関の政策

米国では、過去数回の大停電が発生している。

1965 年 1 月： アイオア州と中西部5州の一部⇒2時間の停電。200 万人へ影響。
1965年11月： ニューヨーク州、マサチューセッツ州などの北東部8州⇒最長13時間30分の停電。400 万世帯へ影響。
1965 年 12 月 テキサス州、ニューメキシコ州、メキシコ⇒2 時間の停電。100 万人へ影響。
1977 年 7 月： ニューコーク州全域⇒最長2 5時間の停電。900 万人へ影響。逮捕者 3766 人。
1989 年 3 月： カナダ･ケベック州⇒最長9時間の停電。
1996 年 8 月： 米西部⇒最長5時間の停電。
2001 年 1 月： カリフォルニア州⇒輪番停電。200 万人へ影響。

これらの共通する要因としては、

1）樹木管理の不備
2）系統状態の安定限度検証の不備
3）緊急状態の認識と緊急マニュアルの欠如
4）人材教育の不十分さ
5）米国における系統全体図の把握能力欠如

等が挙げられるが、今回の情報通信システム上の監視システムトラブルでは、新たな問題が発見された。

2003 年 10 月 15 日、NERC は再発防止にむけて制御地域や信頼度コーディネーターに「信頼度確保の為の短期的行動指針」を送付した。前章でも触れたような GE 社のバグは最近の情報であるが、10 月では以下の部分に重点を置いていた。

1）電圧･無効電力の管理（日間管理表）
2）信頼度コミュニケーションの強化（情報連絡の重要性）
3）系統監視制御機能の故障報告書提示/故障状況、バックアップ体制、故障時の運転マニュアル
4）緊急時の行動指針（負荷遮断の権限などを含む）
5）緊急訓練
6）樹木管理

その後、米国とカナダの合同事故調査団が報告書を作成し、メディアに公表している。大停電直後

の米国政府機関の主な活動及び政策は、以下に分類される。

対応事項:

1) 非常事態宣言
2) テロの確認、事実、
3) 安全確保の指針
4) 帰宅、飲水の奨励
5) 市内の随時状況発表
6) 治安維持の警告
7) 停電の原因と状況報告
8) 節電要請
9) 都市機能復旧見通し報告
10) 各連邦、州、市代表の声明
11) 行動アドバイス
12) 市長とＮＹ証券取引所ベル
13) ＮＹ復旧と地下鉄再開情報など
14) 調査報告と事後処理計画発表

上記情報は随時、記者会見やプレスリリースが行なわれた。テレビやラジオのインタビューも多く対応し、メディアニュースに頻度も多量であった。市民の求める情報ニーズには十分な頻度であった。重要な情報は、その問題が不安解消もしくは解決されるまで提供されていた。頻度やタイミングも大変良く出来ていた。

それぞれの役割と責任に関しても良く判る状況であった。州は「地元と国」「地元間」の調整機能を果たし、停電復旧関連は市よりも発言が多かった。市は市民の身近な立場として、全情報に対応していたが、市民が行うべき対応措置に重点を置いていた。連邦はテロ関連の声明に重点を置いていた。

6.4 我が国における大停電時の影響

前章では北米大停電の状況と影響を述べたが、日米の電力供給と環境の相違から考察する。

我が国の電力系統はシンプルであり、運用及び管理会社などは1社運営になっている。電力会社間の交流変換もシンプルである。自由競争激化に伴い人的教育やセキュリティ、保守にかけるコストの軽減は日米共通の問題であり、設計の一部やオープンソースの活用を外部委託している部分も共通する。裏を返せば、脆弱部分の発見は他者から行われる可能性もある。

建設やリフォームに関する基準も老朽化しており、データ多重保存や核シェルター導入などの経費の捻出も容易ではない。しかし、こうした問題点は、国際的な技術交流や行政の補助で改善する事ができる。早急な検証と対策が必要である。

万が一、我が国でサイバーテロやサイバー犯罪が発生し、電力網が遮断されたらどうなるであろう。東京においては、ニューヨーク州以上の影響が推測される。

懸念材料を以下に列挙する。

1) 緊急体制が確立されていない
2) サイバーテロのシミュレーションのよる検証がない
3) 国民的危機意識が乏しい
4) 災害時の知識が乏しい
5) 情報提供源の確保が未完成
6) 情報収集体制が未熟
7) セキュリティポリシーの認識が希薄
8) 国際的技術交流が少ない
9) 電力業界の閉鎖性が信頼性を欠く
10) 監督官庁の権限が明確ではない (国民の未認識)
11) 過去の停電時による教訓が乏しい
12) 災害マニュアルの未整備

.

7. 我が国でのサイバーテロの可能性

7.1 電力インフラに対するサイバーテロの可能シナリオ

まず電力インフラを対象とする攻撃者は、制御システムを攻撃することを考えるであろう。広範な地域を網羅する制御システムでは、しばしば遠隔施設が無人であり、物理的な監視設備も置かれていない。このような施設では、物理的な侵入によって制御ネットワークへの接続が簡単に行われてしまう危険性がある。認証や暗号面でもハッカーの侵入リスクが存在する。

想定されるテロ組織は、国内潜入チームが数人単位で存在し、それぞれ諜報・偵察・ソーシャルエンジニアリングを担当するチームと、専門技術に特化したチームに編成すると考えられる。

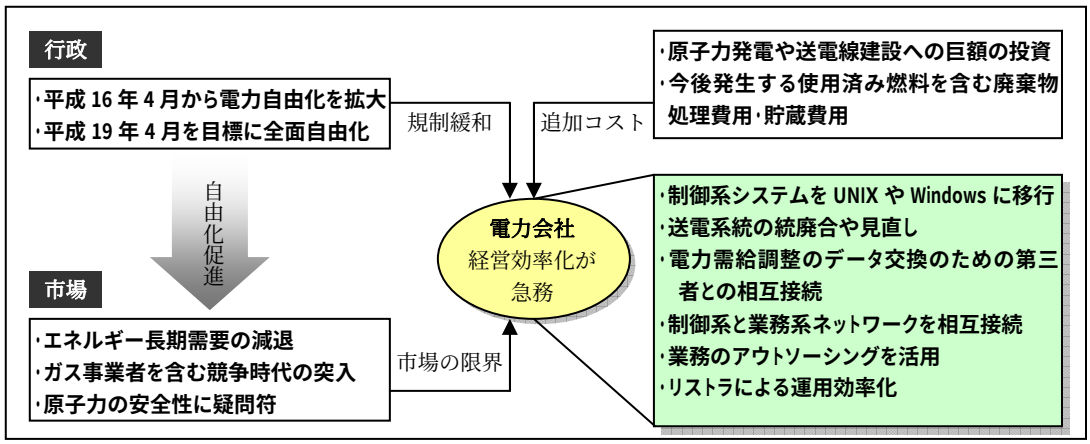
これらのチームは予め日本国内で十分な下調べを行い、攻撃対象に対しての詳細な情報を得るだけでなく、内部に詳しい人物とも接触して買収あるいは脅迫を行う可能性もある。米国の机上演習「Digital Pearl Harbor」では、ある程度の資金を投入することで内部の人間を買収することが可能との見解を示している。内部者を抱き込むことで事前に機密情報を入手するだけでなく、それを脅迫の種にしてテロ実行日には不正操作の協力をさせるというシナリオが考えられる。

各 cell[1] は国内においてテロリーダーの指揮の下に独立して行動し、cell 間相互の連絡や協力体制はない。これは、仮に1つの cell が捜査当局に拘束された場合でも、他の cell が連鎖的に摘発されることを防ぐ狙いがある。海外のハッカーチームはテロリーダーが最終的に収集した重要インフラについての詳細な機密情報を分析し、攻撃方法やその際のツール等の試験を経た後、他の国もしくは自国内の同等の重要インフラ施設に対して模擬的な侵入を試みる可能性がある。

【1】組織細胞。テロ組織の最初単位のチームまたは班の意味として使われる。

7.2 電力インフラの脆弱性

我が国の電力産業の将来像と問題点



我が国の電力事業を取り巻く行政や市場環境も、欧米化にみられる自由化の流れの中で類似の状況がみられる。特にエネルギーの 90%以上を海外に依存する我が国は、エネルギーの効率化のために原子力発電に注力している。しかし、景気低迷で電力需要が減速する中、今後のその使用済み燃料の処理や貯蔵にかかる費用を考えると、電力会社は来るべき自由化の本格化を前にしてかなり大幅な投資抑制・コスト削減計画を推進しなければならない事情がある。こうした自由化の流れから、我が国の電力会社も欧米と変わらず共通の脆弱性を抱えることになる。

サイバーテロおよび物理的攻撃によるテロを含めると、我が国において考えられる攻撃対象は以下の施設のいずれかもしくは複数である可能性が高い。

●原子力などの主要発電所に対する物理的攻撃
●基幹送電線に対する物理的攻撃
●変電所、配電所などへの物理的攻撃
●マイクロ無線装置や施設への物理的攻撃
●中央給電指令所（電力本社）への物理的攻撃

7.3 サイバーテロの被害予測

8.14 米東部大停電のような事態が我が国の首都圏を直撃した場合、その経済損失は単なる（計画）停電の場合とテロ攻撃にあった場合とで大きな差が出てくると思われるが、総じてニューヨーク地区の経済的被害を大幅に上回る損失となるであろう。

米大停電における最も大きな被害の1つは冷蔵の必要な生鮮材料の腐敗による被害であり、停電自体の影響とテロの可能性などから JFK 空港も一時的に機能停止に陥った。また、多くの企業の工場停止に追い込まれており、例えば自動車大手フォードは 44 ヵ所の工場のうち 23 ヵ所を一時閉鎖した。以上のことから、改めて大都市圏が過度に電力インフラに頼っていることが伺える。

米国の大停電（3～4 日間）の経済損失は、各会社の概算によって幅がある。算出方法はそれぞれのタイムスパン（日毎）における損失額を独立的に産出し、その合計によって総合的な額を導き出している。経済損失項目としては直接的な機会コスト（経済活動の停止）、間接的な機会コスト、冷蔵材の腐敗コスト、政府による停電対策コスト、電力会社の復旧コストなどに分類され、損失額幅は合計 40 億～100 億ドル（約 4200 億～1兆 500 億円：1ドル=105 円換算）まで多岐にわたる。[1] 筑波大学教授の内山洋司氏によると、ニューヨーク大停電は最初の2日間で 40 億～60 億ドル（約 4200 億～6300 億円）の経済損失が見積もられているが、関東圏でも発生すれば（少なくとも）同程度の被害が予測されると述べている。[2] また、電力中央研究所の浅野幸志上席研究員は、2003 年 7 月に原子力発電が停止するシナリオとして首都圏の一般家庭 120 万～130 万世帯が約 144 時間（6 日間）停電の影響を受けた場合、6200 億円になると換算している。

しかしながら、米大停電の場合は主に3日間の停電期間のみに焦点を当てた算出方法を取っており、将来的な影響度については考慮されていない。実際にテロが起きた場合、物質的な破壊被害や二次テロを防ぐための治安維持に必要な政府出費に加え、長期的にはテロに狙われたことによる一般市民の不安から来る消費の抑制、そして海外投資家によるリスク分散のための投資額の流出、連鎖的に起きる株式市場の大幅な減速、観光客離れなど旅行関連業界を筆頭とするサービス業界の低迷、政府だけでなく大手企業や重要インフラ企業によるテロ対策の導入コスト、そして景気減速による失業率の増加とリセッションの可能性などを踏まえると、長期的な視点でみた場合に、我が国に及ぼされる経済的な被害は、単なるソフトウェアのバグが原因であった米大停電の比ではない。

そこで今回は、仮に首都圏においてテロの原因による停電が3日間続いたと過程した場合、まず営業活動ができない 3 日間の機会コストについては、以下の計算をした。

日本の GDP 約 400 兆円 X 首都圏の GDP 比 40% X（3 日間 / 365 日）= 約 1 兆 3200 億円

【1】”Northeast Blackout Likely to Reduce US Earnings by $6.4 billion” AEG 2003/8/19
“The Economic Cost of the Blackout” ICF consulting
【2】2003 年 10 月「原子力の日」記念シンポジウム

しかし、首都圏とは1都 7 県を含むため、そのすべてがテロ被害に遭うのは非現実的である。特に首都湾岸地域の火力発電所は送電網が停止した際にフル稼働で対応できると過程した場合、仮に広範な地域の送電網系統が物理的に破壊されたとしても現実的に見て 40～50%の電力が足りなくなる程度だと予想される。以上の推測を基に東京圏を中心とした停電では1兆 3200 億円の約半額が妥当だと思われる。

一方、冷蔵材の腐敗被害は、米大停電の情報を基に機会コストの約 4 分の 1 程度とし、政府の対策費用はテロ被害を想定して米大停電時におけるニューヨーク州の支出の約 2 倍の額を基準とした。また、電力会社によるインフラ復旧コストは物理的な破壊を伴うため、テロ対策のための特別費用を含めて米大停電の費用の約 4 倍程度に設定した。上記の条件を当てはめた数値が下記の通りである。

首都圏の被害による経済損失額 (3 日間)

	損失項目	金額
直接的な損失要因	収益の機会損失	6,600 億円
	冷蔵材の腐敗	1,650 億円
	テロ被害復旧費	50 億円
	電力事業者の復旧費	2,000 億円
	政府の特別対策費	400 億円
小計		1 兆 700 億円

今回の重要インフラにおいて、重要な鍵を握る電力会社との協力体制は不可欠であり、その後の国民への信頼構築と危機意識の啓蒙」を官民一丸となって実施することが、重要なテーマであると思われる。

前述したように一極集中の東京圏を狙ったテロ要因による影響と長期的な経済低迷を考えると、その実質的なインパクトは数十兆円から数百兆円にさえ換算される可能性も否定できない。

8. 重要インフラ対策の基本計画策定

8.1 e-Japan 構想における我が国の位置付けと理想姿勢

首相官邸のWebページを見ると、1994 年に高度情報通信社会推進本部を設置し、実に 6 年の歳月を過ぎた 2000 年に情報通信技術戦略本部とIT戦略会議を設置している。以下に設置の基本方針 6 箇条を抜粋する。

⑴ 政府は、これまで「高度情報通信社会推進に向けた基本方針」及び「アクション・プラン」に基づいて、我が国の情報通信の高度化に資する施策を着実に推進してきたが、アクション・プラン策定時以降の状況変化や新たに生じた課題について整理する。

⑵ 我が国においても、インターネットの爆発的普及、携帯電話等の加入数が5千5百万を超える等、情報通信が経済・社会の諸分野において急速かつ広範に浸透してきており、情報通信関連産業は新たなリーディング産業となりつつある。この情報通信を通じた社会、経済の変革を成功させることが、来世紀における我が国の繁栄を確実なものとする上で必要不可欠となっている。

政府としては、経済フロンティアの拡大、高コスト構造の打破、活力ある地域社会の形成や真のゆとりと豊かさを実感できる国民生活等を実現することを目指している。

また、我が国の活力を維持していくためのツールとして情報通信を最大限活用することが重要である。

一方、本年1月下旬には行政機関等のサーバに対する攻撃が起きる等、高度情報通信社会の安全性、信頼性に対する懸念を生じせしめるような出来事も発生しており、政府としては高度情報通信社会の発展を阻害しかねないようなこれらの問題に対しても迅速・的確に対処していく必要がある。

⑶ 以下の 5 つの項目については、高度情報通信社会を構築するに当たってのその重要性、緊急性に鑑み、特に優先的に取組むこととする。

①電子商取引の本格的普及
②公共分野の情報化
③人材の育成及び情報リテラシーの向上
④高度な情報通信インフラの基盤整備
⑤ハイテク犯罪・セキュリティ対策

⑷ また、教育の情報化や電子政府、IT21 (情報通信技術 21 世紀計画) といった重要性・緊要性の高い分野については、内閣総理大臣が自らミレニアム・プロジェクトを決定した。加えて、平成 12 年度末より1年間、地方公共団体、民間企業、NPO 等の幅広い参加を求め、「インターネット博覧会 (インパク、

楽網楽座)」を開催する。我が国インターネット利用者層の幅広い拡大を目指すとともに、2001 年の新世紀の門出を祝い、新しい世紀の技術、産業、国民生活の盛り上げを図っていく。

⑸ 更に、ITの急速な普及・活用は、経済に与えるプラスの影響が非常に大きい一方、いわゆるデジタル・デバイド(情報を手に入れることができる者とできない者との間に生じる経済格差)の問題が生じており、この克服が新たな政策課題となってきている。情報通信分野の進歩が、社会・経済に対し急激に大きな変化をもたらしており、この問題を始めとするITの急速な発展に伴う問題に関し、首脳レベルで大きく取り上げられる見込みとなっている。

⑹ 以上に示した通り、社会・経済における情報通信の重要性が日増しに高まっている上、この分野における変化は極めて激しい。このため、高度情報通信社会を構築するに当たっては、硬直的な取組みではなく、情勢変化に柔軟且つ機動的に対応していかなければならない。

また、以下のように今後の課題事項を見ても、「経済促進と利便性」「知識の向上」などポジティブプランに重点を置いているのが判る。15 ヶ条の中で、犯罪などの脅威に対する部分は 2 ヶ所だけであり、その対策内容も「情報セキュリティ関係省庁局長等会議」の設置から始めている。以下に我が国政府が提示した今後の課題を列記し、方向性と姿勢を見ていく。

1) 電子認証に関する制度整備

2) ビジネス方法の特許の適切な保護

3) 個人情報保護

4) 電子商取引推進のための制度等の見直し

5) 行政の情報化

6) 高度道路交通システム(ITS)の推進

7) 地理情報システム(GIS)の整備・相互利用の推進

8) 高齢者・障害者の情報通信利用の促進

9) 教育の情報化

10) オンライン接続禁止条項の早期見直しの要請

11) インターネットの総合的技術基盤整備

12) 第三世代移動通信システム (IMT-2000) の導入

13) 低廉な利用料金の実現

14) 不正アクセス対策法制の整備

15) 情報セキュリティ対策

本案件である「重要インフラ防護演習」は、最終事項に掲げた上記の 15) 情報セキュリティ対策項目に入る。

この「情報セキュリティ対策」としては、情報セキュリティ関係省庁局長等会議を設置し、関係省庁で協力して、ハッカー対策、サイバーテロ対策、法的な課題といった広範な課題に取り組むことを決議している。2000 年 1 月 21 日には「ハッカー対策等の基盤整備に係る行動計画」を決定している。この行動計画は、官民を通じ我が国全体において、情報化・ネットワーク化の進展に見合った、適切な情報セキュリティ水準を確保するための基本的な考え方や具体的措置を明示しており、以下のような柱を発表している。

①電子政府の構築を見据え、政府自らのセキュリティ水準を向上すべく、各種対策を実施すること（それぞれのタイムスケジュールを定める）。
・セキュリティに関する信頼性の高い政府システムの構築
・監視・緊急対処体制の整備・強化
・総合的・体系的な情報セキュリティ対策の検討
・民間の人材の積極的活用を含めた人材の育成・確保
②金融、エネルギー、情報通信等の民間重要インフラ等に係る取組みを推進するため、「サイバーテロ対策に係る特別行動計画」を平成１２年内に策定すること。
③国際的連携を強化すること。

その後、約 11 ヶ月を経た 2000 年 12 月 15 日に「重要インフラのサイバーテロ対策に係わる特別行動計画」が決定され、さらに 10 ヶ月を経た 2001 年 10 月 10 日に「サイバーテロ対策に係わる官民の連携・連帯体制について」が決定した。

重要インフラのサイバーテロ対策に係わる特別行動計画の目的等は、以下のように発表されている。

1 目的

いわゆるサイバーテロなど、情報通信ネットワークや情報システムを利用した、国民生活や社会経済活動に重大な影響を及ぼす可能性があるいかなる攻撃からも重要インフラを防護する

2 対象とする重要インフラ分野

情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス （地方公共団体を含む）

3 官民におけるサイバーテロ対策

⑴ 被害の予防 （セキュリティ水準の向上）

被害を予防するため、その前提として、対象となる重要インフラの情報システムのリスク分析を行い、情報システムの重要度に応じた対策を講ずることによって、恒常的に各重要インフラ分野のセキュリティ水準の向上を図る

⑵ 官民の連絡・連携体制の確立・強化

セキュリティ情報（セキュリティ改善に必要な情報）及び警報情報（サイバー攻撃の発生情報等の警戒や緊急対処に必要な情報）の共有、予防・対処等を連携して行うための官民における体制の確立・強化を図る

⑶ 官民連携によるサイバー攻撃の検知と緊急対処

各重要インフラ分野においてサイバー攻撃を受けた場合又はそのおそれがある場合の対応策を定めるとともに、官民全体で対処能力の強化を行う

⑷ 情報セキュリティ基盤の構築

サイバーテロ対策を進めていくため、人材の育成、研究開発、普及啓発、法制度の整備等の情報セキュリティ基盤の構築を推進する

⑸ 国際連携

サイバー攻撃は、国境を越えて行われる可能性があることから、このような攻撃に適切に対処するため、国際的な連携を推進する

4 行動計画の見直し

この行動計画は、官民の連絡・連携体制の確立を中心として取りまとめた初めてのものであり、政府は、この進捗を踏まえ、定期的及び必要に応じ見直しをする

また、総務省における緊急テロ対策の実施状況(情報通信関係)は、以下の概要になっている。

（出展）情報セキュリティ対策推進会議（平成 12 年 12 月 15 日）

平成 14 年 3 月末現在

情報通信関係	主要な電気通信事業者に対して、サイバーテロ対策を含めた施設・ネットワークの保安確保措置の徹底を図るよう要請	①主要な電気通信事業者に対して、ファクシミリ文書により要請（H13.10.8） ②緊急テロ対策本部決定を踏まえ、改めて公文書により要請　(H13.10.9) ③米国政府からのテロ攻撃予告情報を踏まえ、ファクシミリ文書により要請（H13.10.30）
	主要な放送事業者及びケーブルテレビ事業者に対して、サイバーテロ対策を含めた施設・ネットワークの保安確保措置の徹底を図るよう要請	①NHK、民法キー局、主要なケーブルテレビ事業者及び（社）日本民間放送連盟に対し、放送システムの安全性・信頼性の確保について緊急要請（H13.10.8） ②以下の放送事業者等に対し、「放送システムの安全性・信頼性の確保について」文書により要請　(H13.10.9) NHK 及び放送大学学園/地上系一般放送事業者（193 社）/BS テレビジョン放送事業者（8 社）及び BS 受託放送事業者（1 社）/（社）日本民間放送れ名及び（社）日本ケーブルテレビ連盟
	NHK に対して、国際放送を通じた在外邦人への情報提供等に努めるよう要請	NHK に対し、「国際放送を通じた在外邦人への情報提供等について」文章により要請　(H13.10.9)
	国内テロ対策に関連した電波監視体制の強化	総合通信基盤局において、主な航空用の無線通信について 24 時間の自動記録を実施するとともに、緊急時の連絡体制を強化
	国際電気通信事業者に対し、アフガニスタン及びその周辺諸国との間の国際通信回線の確保の要請	①国際通信を取り扱う主な電気通信事業者（4 事業者）に対して、ファクシミリ文書により要請　(H13.10.8) ②緊急テロ対策本部決定を踏まえ、改めて公文書により要請　(H13.10.9) ③米国政府からのテロ攻撃予告情報を踏まえ、ファクシミリ文書により要請（H13.10.30）
	非常時における無線通信の確保	全国の総合通信局に対し、非常無線通信の確保及び臨機の無線局免許を徹底するよう改めて電話で指示
	サイバーテロ防止のための高機能ネットワークセキュリティシステムの整備	サイバーテロ防止のための高機能ネットワークセキュリティシステムを独立行政法人通信総合研究所に整備し、サイバーテロへの対処能力を強化
その他	サイバーテロ対策 （省内システム関係）	①総務省情報セキュリティポリシーの策定　(H13.2) ②ファイアウォールの強化、ウイルス対策強化　(H.13.1) ③省内システムに対するサイバーテロ等の 24 時間監視　(H13.1)

今後は更に権限と役割を明確化し、、サイバーテロが発生した場合の2次的な被害対策にも注力するべきであろう。国民の危機意識と日常の準備が必要であることを啓蒙し、発令権限に関する規定を整備するべきである。

米国のペンタゴンは 1998 年 3 月に「米国史上最も執拗且つ深刻なサイバー攻撃」を受けた。これに対し、コードネーム「Moonlight Maze」と名付けられた調査が現在も続いている。この攻撃を仕掛けたハッカーグループは、精巧なハッキングツールを使用して NASA、ペンタゴン、政府機関、大学及び研究

施設の数百台のコンピュータをハッキングする事に成功した。盗難された情報の中には技術研究資料、契約書、暗号技術、軍事戦略システム資料が含まれていた、この事件以降、米国諜報機関は最大規模の調査に着手し始めた。調査開始 3 年後の現在でも、判明した手掛かりは極小である。攻撃自体は、ロシアを拠点とした 7 つのインターネットアドレスより仕掛けられており、ロシア政府に対して、攻撃基点の電話番号などを提供、調査、処理を要求している。ハッカーは何回も侵入し、データを盗むようにバックドアを仕込んでおり、システムの中に特定の交信が転送されるようにツールを残していた。しかし米国の頭脳を集結しても、「誰からの攻撃なのか」「どんな情報を盗んだか」「最終目的は何か」「官民を含むハッキング被害はどれだけ拡大しているのか」「脆弱なネットワークシステムを破壊できるツールは残っているのか」等が判明していない。しかも、Moonlight Maze は、単なる序幕に過ぎないと語られている。

米国政府は情報戦に負けることは戦闘能力そのものを失い、国家の崩壊を助長するという認識を持っている。数十億ドルをも費やして配備したミサイルも、情報攻撃による管理ソフトや情報インフラへの攻撃及び破壊で無意味になってしまう。また、開発段階のミサイルの設計･製造記録を改竄する事で開発を遅延させたり、停止させたりする事もできる。こうした修正、修復のコストに膨大な費用と人材が再投入されるであろう事実も認知している。

こうしたサイバー攻撃に対する脆弱性テストは、前章でも述べたように米国では既に 1997 年 7 月にコードネーム「Eligible Receiver」として作戦を遂行している。この演習で、ハッカーがボタン 1 つで都市の電源を切り、緊急対応を不能にする事が証明された。続いて都市機能が麻痺し、社会的混乱が発生する事をも確認した。演習に参加した優秀なハッカーは、世界で最も強固であると自負していたペンタゴンのコンピュータネットワーク110 万のうち 41000 を攻撃し、36 のコンピュータ侵入に成功している。しかも、36 のコンピュータ侵入で検知された報告は 2 例だけであった。模擬ハッカー達は、一度侵入した経路から何度も侵入し、ネットワークを自由に往来しデータ破壊、改ざんを行っている。また指揮命令系統への侵入で虚偽の指示やニュースを送り、混乱と不信感を招く事にも成功している。更に、こうした攻撃は一般的に入手可能なツールのみを使用して参戦していた。

次に参考すべきは 1999 年 10 月の演習 Zenith Star である。電力供給発電所を標的にし、電話回線がパンクするようにコンピュータにデータ負荷を与えた。これにより、政府機関と電力会社などの重要インフラの危機管理体制が脆弱である事を露呈させた。詳細は、前章で述べた通りである。

ハッカー攻撃の単独犯が経済活動を麻痺させる行為は「サイバーテロなのか」「サイバー戦争なのか」の議論は尽きない。従って、この議論は防衛論でとらえるべきかは別問題としても、情報技術力や防衛技術力の長けている米国であっても、完全な防衛は困難であると考えていることを我が国も認知すべきであろう。米国は、今なお絶え間ない演習と膨大な予算、権限の見直しなどを行っている。

東京のサイバーテロによる経済損失は、天文学的な数字になると思われ、被害が発生した場合の国際批判や裁判は免れない。2001 年 10 月 8 日、小泉首相が演説した緊急対応措置に下記の項目がある。これを下に、早急な国際的分析家と共に対策を講じるべきであろう。

1) テロ関連情報の収集･国際協力の強化

2) 世界及び日本の経済システムに混乱が生じないよう、各国と協調し措置を講ずる

がある。我が国は、国民の損益を崩壊しない為の対策を念頭に、早急なサイバーテロシュミレーションを行うべきである。

8.2 情報共有体制の有り方

サイバーセキュリティ対策やサイバーテロ対策において、最も重要であるのが「情報収集」「情報分析」「情報交換と配信」である。サイバースペースにおいての国境はなく、情報技術時代への突入は利便性と凶器が 24 時間存在する世界である。しかも、その「利便と凶器の両羽の刃」は世界中の人間が持ち、経済や政治など社会全体に影響する。

情報化時代は２１世紀の戦争の形を大きく変化させ、軍備、防衛インフラ及び国家経済に多大なる影響を生み出している。その結果、サイバースペースは新しい国際ツールとなり、個人と国家の利益を左右するようになった。。防衛の世界では情報戦争（サイバーウオー）が俄かに研究テーマとして踊りだし、最近発生したイスラエルとパレスチナの数百年に亘る紛争にも、サイバー戦争という分野が登場してきた。2000 年 10 月から 2001 年 1 月まで、双方は 250 以上のＷｅｂサイトを破壊しあった。この被害は両国間の国境を超え、多くの外国企業や団体のコンピュータネットワークまで波及している。

現在、サイバー技術の最も優れた国が最も弱小な国になってしまう危険性を孕んでいる。反対に、膨大な軍事費や人材を投入しない戦術が出現してきた事で、弱小と思われてきた国が世界に踊りだすようにもなった。

こうしたパラダイムの変化に対応していく為の情報戦略は、「官民連携」「省庁間連携」「国際連合的」に討議されなければならない。今後は、情報収集と分析体制の具体的な指針や教育を行うと良いであろう。

我が国は、経済大国世界第 2 位の威信を掛けて「経済安全保障」の目標を共通課題とする。これは、閣僚及び官僚のみならず国民全員の意識として啓蒙すべきである。「危機意識と自己防衛論」を啓蒙することが必要である。こうした社会の体制を目標にする事が積極的な官民連携と情報共有感覚を促進させると思われる。

では、具体的に情報収集のネットワークはどのように考えるべきであろうか。ネットワークとは、下記の原則で構成される。どの原則も、我が国が直面している多様な脅威の特徴を反映している。

1. 情報は分権化させ、ユーザー間で直接取り扱う。また、メインフレームやハブアンドスポークのモデルではなくネットワークモデルに応じて管理方法を決定する。
2. 統一したネットワークのポリシーを施行し、許可及び禁止されているアクションを明確にする。
3. 政府の方針は、保護に焦点を定める。
4. 脅威に関しては、国内外の境界線はない。国内と国外という区別から生じるブラインドスポットや政府機関同士の溝を生んではならない。同時に、情報の収集と使用を国内外で区別していた従来

の「国境での境界」に代わる新しい規則を早急に制定し、政府機関により国民の自由が侵害されることを防ぐ。

5．ネットワークは、政府だけでなく、各行政、民間企業により構成されている事実を反映して構築する。

6．民間企業が有する情報も政府が効果的に使用できるネットワークに構築する。

7．脅威との戦いは、我々の生活と価値を保護するための長期に渡る取り組みである。ポリシーの施行や対策の実行には、国民の支持と信頼が不可欠である。国民のプライバシーや自由は保護されなくてはならない。

これらの原則は、どのように実現するべきかを下記に記す。

第一に、政府は情報の共有と分析に重点を置く。

情報へのアクセスを厳しく制限するシステムが開発され、情報の参照には「知る必要がある」ことを証明する特定の情報が必須であり、最初に情報を入手した機関による許可も必要であった。このシステムは、ある情報を知るべき人物を、先天的に決定していたと考えてよい。これは情報の共有により生じる利益よりも、不注意もしくは故意に情報が漏洩するリスクの方が高いという判断に基づくものである。このような構造と意識は、我々が現在直面している問題には不適切である。

2001 年 9 月 11 日の事件は、情報の共有方法が適切でなかった事実を浮き彫りにした。行政縦割りで情報を守秘し、個々でも情報を閉鎖していたことが問題なのである。政府は、民間企業にもシステムを公開し、情報だけでなく技術や資金へのアクセスも可能にするべきである。必要であれば運用方法を再検討し、双方向の共有と相互運用性を提供する技術構成及びツールを採用する必要がある。また、情報を収集した機関、使用するユーザーのニーズにも配慮した上で、情報の提供を制御するのか、するのであればその方法を決定する。こういった決定は、機密情報のセキュリティが確立し、個人情報が保護されている環境で行うべきである。

また、政府は、個人が有する情報も効率的に利用する必要がある。ただし、規則とガイドラインを適用しているシステムのみに限定し、国民の自由を保護しなければならない。テロリストによる攻撃対象を国家が判断することは不可能である。だからこそ、情報を駆使して攻撃の検知、防止、対応を行わなければならない。政府がテロリストである可能性があると判断した人物の、旅行、宿泊、財政、移住、保険、学歴などの記録は、その人物の行動や個性だけでなく、他のテロリストの行動や個性の判断材料となる情報を含むことが多い。しかし、情報への正当なアクセスと使用を判別する一貫したガイドラインを政府が立案し公の場で論議されるまでは、プライバシーの侵害に対する不安は払拭されないであろう。これは情報利用と運用プログラムに必要な新技術の開発の妨げとなる。

考えるネットワークの構築は、今まで以上に急を要するものである。テロリストは今も世界中を脅かし

ている。テロリストにより大量破壊兵器が使用される可能性も高まっている。技術基盤の構築、機関意識の改革、新規則と手順の策定、必要財源の確保は、どれも容易に達成できることではないが、ネットワークを利用する全ての人々を統治し、自由を守るためのガイドラインに沿って管理されるネットワークの構築を、行政機関に望まれる。

テロ行為を予知して防止するために政府が把握、分析、共有、対処すべき特定の情報が存在するという具体的な状況を想定して調査を行い、シナリオベース検討されるべき点を把握した。

1) どのような情報が分析され、共有されているか
2) 情報の共有を妨害しているものは何か
3) システムに配備した全センサを活用し、情報の収集量を増加するには、どこに情報を提供したら良いか
4) 機密情報（情報源など）の漏洩を防ぎ、且つ利用する情報をネットワーク全体に供給するにはどのような手段を講じるべきか
5) どのプロセスを変更し、どのような新技術を開発すれば分析と情報の共有が改善するのか
6) テロ行為を示唆する情報を識別し、共有する一方で、どのようにしてシステムのフラッディングを防ぐのか。

提案するネットワークコミュニティとは、最高の技術を駆使して情報と意見の共有を確立し、国土のセキュリティを保護するものである。同時に、政府はあらゆる手段を講じてテロ行為に立ち向かっているという信頼を国民から得なければならない。実用的なポリシーのガイドラインに沿って構築し、ポリシーはネットワーク全体に適用し、情報の収集、分析、共有、使用が許可されるものと禁止されるものを明確にする。

また、官民が連携し、有用な情報を提供し共有する。ネットワーク自体の目的は、情報を分析して有用できる人物に提供すること、そして規則とガイドラインが整ったシステムから個人所有の情報を提供することにある。このネットワークコミュニティが目指すのは、政府の「センスメイキング」能力を高めることである。センスメイキング能力とは、莫大な量の情報の中からテロ行為のサインを識別する能力と、テロ行為かの判断、テロ行為の防止もしくは対応にあてる時間を生み出す能力である。

だが、このような変化が必要であっても、国民の信頼をなくして達成できるものではない。プライバシーと権利が保護されていること、企業に対して無関係な情報や無意味な情報が不当に要求されないこと、納めた税金が正当に使用されていること、そして何よりもネットワークにより我々のセキュリティが保護されているという信頼が必要である。

ネットワークコミュニティを構築するために解決すべき課題は莫大である。ポリシー、プロセス、技術の使用方法など全てを変えなくてはならない。そして文化や意識といった何よりも改革が難しい無形資

産を、根本から変える必要がある。我々が考える種のネットワーク構築を妨げるのが、この無形資産である。様々な政府機関や民間企業から指導的役割となる環境が生まれ始めている。今必要なのは、動き始めた試みを促進する計画と、目標に到達するための議論と合意である。

本報告書で打ち出した指針に基づき、我が国全体で情報共有の改革を開始するために、中間的機関や公共の民間団体を設立することを提案したい。これらの団体ではネットワークを構成する全ての団体の代表者が指揮をとり、安全なネットワークを構築する国家戦略を打ち立て、基本構造を決定する。政治、組織、技術が絡む複雑な問題であるため、一度に構想を考え構築することは困難であろう。部分的な機能を拡張することから開始し、既存のシステムを効率よく使用して、時間をかけて新しい技術と融合させていく必要がある。このためには、柔軟で順応性がある構造が求められる。

また下記について表明することを提言する。

・国民に関する国内で収集された情報の入手、保持、流布に関して、他の諜報機関、防衛機関、セキュリティ機関が有する権限に関する管理ガイドラインを作成する。
・諜報機関に関する管理するガイドラインを作成し、国内での情報収集に関する必要条件を定める。
・プライバシー保護及びその他の権利を保護する組織を設立する。

政府発令の内容は可能な限り公にする。またセキュリティ情報の目的を体系化した法案の制定を提案するべきであり、下記は実例である。

1) 中間的組織、民間組織を召集し、分権化したネットワーク実現のための方針や概念を確立する。また、1年以内に行動計画を発表する。
2) 各行政、民間機関と協力して分権化した分析センターを設立し、ネットワーク全体とのコミュニケーションを円滑にする。また、デジタル化、保持、情報の共有に関する基準を設定する。
3) 脅威及び脆弱性に関する地方機関からの情報要求に対応するために、明確な機構を設立する。
4) ネットワーク全体で可能な限りの情報を共有できる方法を確立する。共有する情報量に関して機関間で生じる問題にも対応できる機構を確立する。
5) 民間が有する情報の入手、使用、保持、流布を管理するガイドラインが設定、実行されているかを監視する過程を確立し、監視と説明責任を確実なものにする。
6) 行政、民間機関と協力し、情報共有と分析のための目標を設定する。各機関を評価する基準を策定し、定期的に評価を行う。
7) 地方自治体機関と情報を共有する機構を確立する。また、これらの機関と他機関との直接の情報共有を要請する。
8) 脅威及び脆弱性に関する地方自治体機関からの情報要求に対応するために、明確な機構を設立する。

9) 機密でない情報を含め、ネットワーク全体で容易に利用可能な情報を増加する機構を設立する。
10) 未知のテロ行為に対する捜査の際に発生する可能性を考慮したシナリオベースのプロセスを考え、民間機関が必要とする情報のカテゴリーを明確にする。
11) 民間が有する情報の入手、使用、保持、流布を管理するガイドラインが設定し、監視と説明責任を確実なものにする。

また、解決すべき課題の一つは、情報のギャップを埋めることである。行政と地方自治体、諜報機関と法執行機関、民間企業の間には大きなギャップが存在する。米国では、トルーマン大統領の時代に、政府機関に存在した情報のギャップを排除する目的で情報中央局（CIA）が設立された。1947 年の国家安全保障法を根拠法として CIA は設立され、国家の情報活動を統合し、情報の関連付け、評価、普及を任務としている。

現在、情報のギャップは、冷戦時代よりも現代のほうが大きいといえる。テロ対策の状況を考えると、そのギャップは特に顕著である。重要な情報や分析能力が、多くの政府機関に情報として分散している。これに加え、テロリストの攻撃対象となりうる重要なインフラを保護する何千という個人や、テロ行為の防止に有用な情報をデータベースにもつ可能性のある無数の民間企業にも情報が分散している。このような関係者の間に存在するギャップを超えた通信、共同開発、共有がテロ対策には不可欠である。テロ行為の最初の兆候が現れる箇所を予測することはできない。テロ行為が分権的であるという性質を考えると、処理を行い共有すべき情報量は飛躍的に増加し、幅広い分野に渡る。諜報機関や法執行機関、医療介護機関、民間企業、そして情報を受信する関係者全員が、テロ計画の予測と攻撃の防止に常に関係しているというのが現実である。

このように分散している情報を集約することが解決策ではない。集約は、情報分析の分権化につながらないからである。また、情報を集約すると、分散したソースから収集する情報を常に最新の状態に保つことが困難となり、情報の利用価値がなくなる恐れがある。また、ネットワークを構成する全員に情報へのアクセス権を与えることも解決策とはいえない。国民の自由が脅かされ、機密情報が漏洩する危険性が高まる。また、各機関が独自で行動するため情報や分析結果が効率よく提供されない結果となる。実際、データの量が莫大で不要な情報が多く、分析により関連性を発見することが困難な状況なり、地方の機関が適切な保護処置を行うのが極めて困難となる。これを踏まえ、関係する機関もしくは個人が、テロ行為のサインを不要な情報の中から識別できるネットワークを考える。ネットワーク全体から専門家を起用し、本来の職務に必要な情報の収集、アップデート、理解に対して、不要な情報を提供することなく対応する。

さらに、現代の脅威に対抗するには、これまでにない速さで情報の収集、共有、利用を行わなければならない。冷戦時代のように遠方の軍隊の規模や戦略を認識し、海外政府の行状を確認するのではない。いつ起こるかわからず、弱い立場にある国民を標的とした緊急攻撃の可能性を検知して阻止

することが目的である。さらに、狙撃攻撃、自爆テロ、自動車爆弾、ハイジャック、大量破壊兵器（化学兵器、生物兵器、核兵器、放射性物質兵器）、大量破壊（サイバー攻撃）など、攻撃者の数だけ攻撃の種類は多様である。このように多様な攻撃の検知、防止、対応に最も重要なことは時間である。また、警察官も含め、あらゆる水準で決定が円滑に行なわれるように、情報はニーズに合わせて提供されなければならない。

情報共有体制の基本目的は、異なる団体を結びつけるために必要な技術、ツール、インフラ、ポリシー、方法を明確にし、必要な情報のみが迅速に提供される環境を構築することである。情報の共有自体が目的ではない。むしろ、情報の共有は、入手可能な情報の利用価値を最大限に提供し、テロ行為に対する適切な判断と対策を行うためにより多くの時間を提供する手段でしかない。

我々が考えるネットワークを実際に構築するには、次の規則を定める必要がある。
⑴ 情報が有用かどうかはどのように判断するのか。
⑵ システムにとって有用であると思われる情報に関して、誰がどの部分の責任を負うのか。
⑶ 情報へのアクセスを許可する基準は何か。また、どの使用目的が許可されるのか。

さらに、監視と公に対する説明責任についての規則も定める必要がある。

最後に、情報の収集、使用、共有に関するガイドラインも様々な理由から非常に重要であることがわかる。まず、ガイドラインは、ネットワークで収集され、共有されている情報の乱用を防ぐために必須である。乱雑な共有は、国民の自由に関する問題を引き起こす結果となる。2 つ目は、ガイドラインは国家公務員により統括されるべきである。しかし、規則を理解せず世論の批判を恐れていたりする場合は、テロ計画の予測や攻撃の防止に必要な法的行為を実行しない可能性がある。3 つ目に、ガイドラインは、ネットワークの構成員の連携を確実にするために必要である。他の組織と共有している情報に変更があったことを知らされていないと感じた場合、たとえ指示であるとしても情報の共有を行わない可能性がある。最後に、ネットワーク上で特化されている機関で情報が使用されている場合、国民の信頼を得る目的でガイドラインが必要である。つまり、国民は政府が情報を必要とする理由や用途を可能な限り知る必要がある。また、情報が乱用されず、個人の権利が侵害されることはないという信頼が必要である。ネットワークを動作させるコードを書くだけではなく、ネットワークを管理するためのコードも必要である。

シナリオベースの運用

ネットワークを構築するには、最初に運用の方向性を決定する必要がある。システムに情報がどのようにして集まるか、その情報を有用な知識に変えるにはどのような手段を使用するかという実際的な理解に基づいて方向性を決定する。また、シナリオに沿って決定し、ネットワーク全体のユーザーのニーズに合わせて決定する必要がある。政府は、政府機関に対して実行される可能性のあるテロ行為の

シナリオを作成し、実行して、必要となる情報、通信網、情報収集要請、データソース、分析要請、決定過程、応答ニーズ、応答予定表を判断するべきである。このようなシナリオから決定する方向性は、新たな脅威予測や変化するユーザーのニーズに基づき、定期的に更新するべきである。

運用の方向性を定めることで、既存のネットワーク構成に存在するギャップ、単一機関への依存状態、隘路が明確になり、これからのネットワーク構築に必要なものを把握することができる。ネットワークに必要な全ての接続において帯域幅、接続性、記憶装置、共有要求を最小限に抑えつつ、最も効率がよく有用な情報のワークフローを決定する必要がある。また、個々の機関内部での情報技術習得やワークフロー改良の計画を許可する内容でなければならない。また、ネットワーク上の各ノードのレスポンスタイム、データ共有要求、情報品質、責任、権限の基準を示す必要がある。

ネットワークは分権化するべきであるが、設計、構築、管理を担う人物が必要である。関係者を召集してネットワークを設計し、ネットワーク構築に必要な資金の管理を行う役割は、内閣官房が担うべきであると考える。組織内部に管轄がある機関が最も信頼性があり、プライバシーに関連する問題が生じても耐え得るネットワーク構築の先導となると確信する。

情報共有システムには、課題が複数ある。

1. 情報の分析、伝達共に、単一の障害の影響を受けやすい。
2. 上位組織への情報の提供を考慮して構築されており、ネットワーク全体の実行機関への提供が考慮されていない。
3. リアルタイムの動作を適切にサポートしていない。
4. 重要情報のリポジトリの多くは分析ツールとの相互運用性がないため、オンライン上でアクセスして分析することができない。
5. 政府、地方自治体同士の信頼性が不足している。
6. 莫大な量のデータからテロのサインを判断することが困難である。分析ツールが最新のものでなく、データが処理しきれていない。
7. 各機関の情報が活用されていない。
8. 私的な情報の乱用に大きな関心が集まっている。
9. 通報される情報を直接使用することができない。これは、最初に情報を受ける人物に関連情報が日常的に提供されていないためである。
10. 情報の共有と分析に関して、権限と責任の明確な境界が定められていない。
11. テロ行為が発生した場合の動作など、システムの検証が十分行われていない。

多種多様な組織を繋ぐ効率的なネットワークを構築するには、必要な情報の発見を容易にするディレクトリサービスが必須である。場所（重要なインフラ、目印、地理的な資料など）、人物、組織、テロ行為の手段に関する情報や、様々な分野の専門家に関する情報を提供され、同様の問題に対して他の

組織が行っている対策を把握する。ディレクトリサービスには既存の技術を生かすべきである。セキュリティとアクセス・コントロールが整備された、自動化したディレクトリであれば利用が可能である。また、情報を有する組織もしくは人物に、共有できる情報とその提供先を制限する権利を与えるべきである。ディレクトリはリアルタイムに監視、同期され、ネットワークユーザーの技術と興味をプロファイルし、自動的に更新されなければならない。

もう一つ、ネットワークに必要なのは、データとデータアプリケーションを切り離して相互運用性を高めることである。データセットは、目的や基準、言語の相違や、他のデータセットへの書き込みを考慮して作成されていないため、そのままでは相互運用ができない場合が多い。ここで、データディレクトリ、メタデータの基準、XML などの変換基準を導入すると、他機関に存在するデータを把握し、入手することが可能になる（必要な権限を持っている場合）。XML で記述したデータはカテゴリーをフィールドごとにタグで指定できるため、効率よくデータのやり取りをすることができる。相互運用を実現するプロセスも自動化するべきである。ソフトウェアツール（エージェント技術）を使用することにより、ネットワーク全体からデータを検索、検出し、集権化したデータベースへの移動、統合を行わずにディレクトリレベルの情報のみを収集することが可能になる。

また、ディレクトリサービスを使用することで、複数の団体が協力し、情報を共有して共通の問題に取り組むことができる。この結果、お互いに情報を提供するだけでなく、莫大なデータフローを最大限に利用する分析技術を拡大することが可能になる。このためには、全てのユーザーのワークフローでネットワークが使用されなければならない。上記のような理由から、ワシントン D.C.の中央集権型の統合されたリポジトリは実用的ではなく、脆弱であるといえる。我々はまず、前述のようなディレクトリサービスを使用した相互運用可能なデータベースのモデルを立案することから始めるべきである。データを統合（ネットワーク上の様々なソースから適切な情報のみを検出）して分析するためには、ネットワークに様々なツールを導入する必要がある。

さらに、大量のデータを異なる形式（レポート、画像、映像、バイオメトリックデータなど）で容易に移動できなければならない。また、トップシークレットで暗号化されたデータから機密扱いではないデータまで、あらゆるセキュリティ・レベルのデータが共有されるべきである。

様々な機関に情報の共有を求めるには、データを強固に保護しなければならない。アクセス権を制限し、データの使用目的、使用期間を限定する必要がある。また、データの使用は許可を得た人物のみに限定する。このためには、アクセス・コントロール、認証、全面監査といった機能が必要である。情報漏洩の防止や国民の自由を維持するためにも、データ保護は非常に重要な課題である。オンライン認証は、適切な目的を持つユーザーにネットワークの使用許可を与えるために必須であり、その技術は日々向上している。オンライン認証技術の向上によりネットワークセキュリティは進化している。複数のユーザーが信頼できる環境で情報をやり取りし、不正使用の防止及び検知のためにネットワークの

監視が行われている。こういった技術には、チップを内蔵したスマートカード、バイオメトリクス、セキュリティ回路が採用されている。多くの識別技術では、データを匿名化する新たな技術が導入され、プライバシーを確実に保護する対策が採られている。このような保護対策を適所で採用することは、情報の共有を制限することにはならない。逆にネットワークと情報共有のルールに対する信頼性を生み出し、情報の共有を促進すると考えられる。

認証技術は日々進歩しているが、その技術を 1 つ採用するだけで信頼できる認証が確実なものになることはない。クラックが不可能なスマートカードやトークンは存在せず、バイオメトリクスは 100%信頼できるものではなく、複雑なパスワードは記憶、管理、配備が難しい。これらの技術を組み合わせ、人と手順の課題（登録手順や監査証跡など）を克服してこそ認証は信頼できるものになる。よって、システムには複数の認証技術を採用することが望ましい。複数の認証技術を採用する場合は、トークンもしくはスマートカードへのパスワード設定に加え、バイオメトリクス、ユーザー確認のための質問、アクセスプロフィールの適合などで認証を行う。認証は、ユーザーが有する情報を使用し、トークン及びスマートカードで採用し、ネットワークで実行された場合に最も強固なものとなる。クレジットカード会社では認証技術を有効に採用している。トークン（クレジットカード）、パスワード（暗証番号）、ユーザー確認のための質問（「母親の旧姓は？」など）、プロフィールの適合（普段と同じように利用しているかなど）を組み合わせて認証を行っている。

情報権利管理技術（次世代のパーソナルコンピュータ、OS、文書アプリケーションに使用する技術）も、文書レベルでのデータを保護し、ポリシー管理システムを有効に構成する鍵となる。特定の文書へのアクセス権を持つ人物や文書を破棄する時期に関するルールを定め、保存されているデータを保護する高速暗号化が可能なストレージシステムが必要となる。

不変的な監査（不正操作が不可能なネットワークアクティビティログを保持する技術）と追跡も信頼性を高めるために重要な要素である。情報の提供元、アクセスした人物、使用目的を追跡することにより説明責任が円滑になる。監査技術により監視も円滑に実行でき、強固なセキュリティを配備することができる。また、不正なアクセスや情報の不正使用の防止も可能である。セキュリティ監視センターでは、データ使用状況を常時監視して、ポリシー違反や不正使用の可能性がある場合は監視員に通知するツールを使用する。このようなツールでは、速達郵便の追跡と同様の技術を使用して情報の流れを把握することも可能である。高度な監査技術と追跡技術を備える利点は他にもある。このような技術により、情報の実際の依存関係が明らかになるという点である。例えば、1 つのデータポイントから複数の分析が行われ、後にこのデータポイントが誤りであったと判明した場合、データポイントの依存関係を追跡し、分析者やユーザーにデータが不適切であることを通知することが可能になる。実際に発生した例としては、2002 年にワシントン DC 周辺の狙撃攻撃に関する情報である。関係があるとされたトラックの特徴が誤りであり、警察官は正しい情報ではなく誤った情報に基づき警戒にあたった。その結果、市民も間違ったトラックの種類を警戒していたのである。ネットワークに対する脅威は、内部にも外部に

も存在する。また、不正に使用される可能性も大きい。このため、ネットワーク自体のセキュリティ（物理的なセキュリティ及びサーバ攻撃に対するセキュリティ）とネットワークに存在する情報のセキュリティが最優先課題である。このためには新しい技術だけではなく、信頼できる環境を構築するルールと手順も重要である。信頼できないのに情報を共有する者は一人として存在しない。内部に存在する脅威から保護され、情報の不正使用を防止し、アクセス・コントロールと多元的な認証を備えたシステムでなければならない。つまり、ネットワークを構成する各システムでセキュリティと情報が保障されなければならない。

ネットワークも、情報の流れだけでなく、要望に応じた情報の抽出や、情報へのアクセス権を付与するユーザーの情報を提供するべきである。民間企業間、政府機関、個人ユーザー、処理装置間での情報の共有をサポートする必要がある。データ要求、情報の公開と参照、ディレクトリ検索、データベースへのクエリ、他のポータルからの情報の検討と統合を、ユーザーが自身の作業環境から実行できるネットワークが求められる。

また、ネットワーク自体にも注意が必要である。既存する分析ツールの多くが参照モデルを基にしているため、送られる要求は非常に高度な要求となる。入手された情報は順次処理されるため特に困難である。ネットワークは、政府による監視対象データに適合する情報やテロ行為の可能性を含む新しいパターンに対して、人間による指示がなくても適宜対応をとらなければならない。

新しいアーキテクチャを一晩で開発することも不可能であり、要件を共通にして全ユーザーに OS のアップグレードを要求することも不可能である。したがって以前から使用されているシステムが新しいネットワーク構成の一部となることは回避できない。また、新しい構造の中でも以前からあるデータはアクセス可能であり、共有される必要がある。従って、政府には、あらゆる形式の情報を使用し、あらゆる形式に変換し、品質を保証して、ネットワークを構成する全てのユーザーに提供する技術が要求される。

A) このようにして情報が共有された場合、大量のデータが送信され、その結果重要な情報が見逃されるというリスクが生じる。この問題に対しては、既存のツールを使用することで改善が可能である。例えば、パーソナライズツール、抽出ツール、カテゴリー化ツールを使用すると、個人のニーズに応じて必要な情報をネットワークから選択することができる。政府はネットワーク全体にセンサを配備し、特定の脅威や個人に適合する情報のみを受け取ることができる。センサは自動的にアップデートされ、常に最新の情報のみを通知する。

ネットワーク構成に関するここまでの記述は、多種多様な組織を繋ぐネットワークを構築するために必要な要素の一部でしかない。組織的で分権されたネットワークを構築するには、ネットワークを構成する組織の構造を改革しなければならない。

情報を効果的に共有するには、情報を扱う関係者の役割、責任、権限が明確にされる必要がある。役割が明確にされない限り、機関同士の管轄問題が生じ、何よりも情報の共有と分析にギャップが生じる。この数十年の間に、民間セクターで保有される個人情報は急増した。売り上げ、クレジットカード、旅行、携帯電話に関する情報を即座に入手することができるようになった。このような情報は、政府機関が不審なテロリストの調査を行う際に、決定的な役割を果たす。

政府はテロリストの潜在的な攻撃を察知するために、民間セクターのデータを使用する際に、容疑がない人物のデータにもアクセスしなければならない場合もあり、国民の自由に関わる重要な問題にある。インターネット技術の発展で、クッキーなどを使用して、個人の行動や興味に関する多くの秘密情報にアクセスできるようになった。さらに、指数関数的な処理速度の増加とストレージコストの低下で、個人の生活に関する情報をペタバイト(約100万ギガバイト)単位で収集することも可能となった。例えば、かつてのスーパーコンピュータの性能は、テラバイトのストレージを備えた現在の64ビットコンピュータをクラスタリングさせることで、デスクトップレベルの価格で実現可能となった。これには、良い点もあるが、悪い点もある。例えば、政府はこのようなコンピュータで、テロリストの情報のやり取りを分析して、進行中の策略を暴くことができる反面、それと同じように、政府は容疑のない個人の生活にまで、侵入することが可能になる。政府はそのようなデータをデータ収集企業から購入する。購入されるデータは、緊急の分析に備えて、あらゆる形式で提供可能である。また、最初にデータをある程度分析して、より特定の分野のデータに分割した「データの小売り」も可能である。政府はそのようなデータを政府が独自に集めたデータ(犯罪歴や諜報機関からの情報)と組み合わせる。それに、プロファイリング技術やパターン解析、リンク分析、指紋分析に加えて、洗練されたデータマイニング技術と「ナレッジマネージメント」ソフトウェアを使用する。そのような技術は、民間企業からハードウェアやソフトウェアとして入手する。データには、事前に一定の意味を持つように構成されたものとそうでないものがあるが、上記の技術を使用することで、特定の個人と個人間の行動パターンやつながりを分析することが可能である。また、まったく関連づけられていない大量の情報からも、価値のある情報を見つけ出すことができる。これにより、幅広い情報の中から、効果的な分析が可能となるのである。

多くの情報はインターネットなどのオープンソースから入手する。その中には有益な情報も多いが、情報の信頼性に欠ける場合もある。政府がそのような情報を利用する際には注意が必要である。政府がどのように市民の自由を侵害せずに、企業にコストをかけさせずに、民間セクターの大量のデータを最適利用できるかに掛かっている。

情報共有体制は多くの関係において、其々複雑である。これは社会的にも慣習的にも多くの是正の上に構築されるべき問題であり、専門家による取組みが必要である。e-Japan 重点計画では、前述したように重点政策 5 分野とのつに「高度情報通信ネットワークの安全性と信頼性の確保」を掲げ、別の項目として 5 つの横断課題が決定されている。

1) 研究課題の推進
2) ITを軸とした新たな国際関係の推進
3) デジタル･デバイドの是正
4) 社会経済構造変化に伴う新たな課題への対応
5) 国民の理解を深める措置

以上の課題をクリアした米国組織を以下に紹介する。これらのプランナーにより多く会い、準備を進めていく事が成功の秘訣だと思われる。今回、下記の中ではNIPCの策定及び創設を成功させたNIPC初代長官に会い、米国政府のサイバーセキュリティの取り組みなどをヒアリングしている。NIPC をFBI内に設立した経緯や苦難なども質問した。また、NIPCやFBIが数多くのISACを設立支援している現状も調査した。

1、NIPC: National Infrastructure Protection Center
現在はDHSに統合。FBIが1998年に設立した、対サイバーテロ組織。
GAOはNIPCの情報が遅い等という事で落第点を付けたが、現在総合的な視点から最高の評価を持つに至る。NIPCには以下のセクションがある。

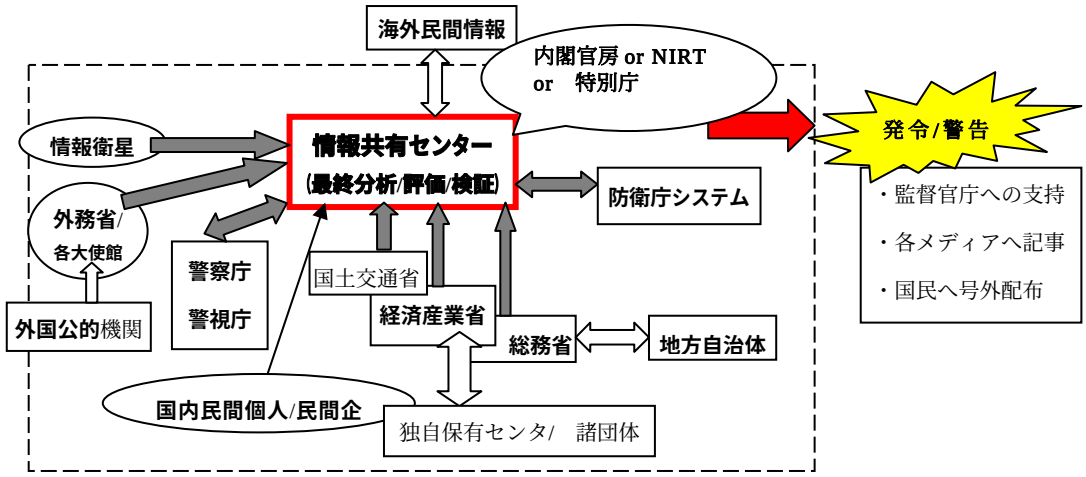
A) コンピューター捜査･運営セクション(CIOS)
⇒コンピューターシステムへの不正侵入に関する捜査支援
B) 分析･警告発信セクション(AWS)
⇒国内外からの物理的脅威及びサイバー脅威の評価･分析
C) トレーニング啓発･戦略セクション(TOSS)
⇒連邦、州、地方警察機関と民間、学会との共同学習と情報交換の場提供

2、PCIS: Partner for Critical infrastructure Security
重要インフラに対する国家安全保障及び経済安全保障を官民連携で活動する調整。
通信、IT, 金融、エネルギーの民間企業CIO達が議案を協議。(例 ISAC設立)

3、CIAO: Critical Infrastructure Assurance Office
現在はDHSに統合。他分野のインフラ計画を1つの安全国家体制に統合する計画策定。
重要インフラのリスク評価。国家教育向上プログラムの策定。
官民セクターにおける重要インフラの防護を目的とした立法策定案の調整。

4、NIAC: National Inftastructure Assurance Counil
政府情報セキュリティ戦略を支援。民間及び海外専門家とのガイダンスなどを計画。
メンバーは30人以下で、全コーディネーターの推薦と大統領指名で決定。

以上の調査から、基本的な下記の日本型情報収集スキームを考えた。



※内閣官房を中心に一元化情報収集体制を構築し、国内のあらゆる有事及び重要インフラ対策にあたる(即時安全保障体制)

8.3 我が国としてのサイバーテロ防護演習の基本計画案提言

先ずは、我が国として、このサイバーテロ防護演習の最終目的を明確に設定する。その設定は、これまでの考察から以下を考えた。

1) 電力事業が保有するシステムの脆弱性検証
2) 電力事業会社及び行政を含む関連各所への緊急連絡の実態検証
3) 国民の重要インフラへの理解と危機意識調査
4) 重要インフラへのサイバー攻撃を想定した政府対応のマニュアル作成
5) 情報共有体制の構想作成（海外のエキスパート混成チーム編成。海外視察。国際会議など）
6) 上記 1) の問題点の改善、対策など実施
7) 上記 2) の反省による緊急マニュアルの策定
8) 上記 3) における国民への問題意識啓蒙⇒メディア、ビデオ、配布物、イベントなど
9) 上記 4) の継続的な審議会の設置提案
10) 上記 5) においては、継続的な国際的活動を実施する

また、電力事業を始めとするライフライン事業全てが「経済安全保障」に係わる事から、我が国の世界における責務は重要であり、こうしたライフラインへの緊急対策と方策は生命運を授ける綱でもある。

下記は日米安全保障において取り交わした日米共同声明である。米国は日本を支援するのみならず、サイバーテロなどの攻撃に関しては、米国経済への影響などにおいて、重要な課題と位置づけている。下記の声明を基に、国際協調を図るのが望ましいと考える。

地球規模のサイバーセキュリティ推進に関する日米共同声明

増加するサイバー攻撃や地球規模の情報ネットワークの相互依存性は、重要情報インフラを守るという挑戦に答える責任を全ての国々に負わせる。日米両国政府は、情報システムとネットワークの安全性と信頼性を確保することの重要性及び「セキュリティ文化」をつくりあげていく世界的なリーダーとしての両国の役割を認識する。この目的に向かい、両国政府は情報システムとネットワークの安全を確保するという課題に関する情報と見解を共有するとともに、サイバーセキュリティ問題に対応する模範例や、効率的なサイバーセキュリティ措置を実施する際の官民連携の重要性について意識を高め、強調することとする。

具体的に、両国政府は以下のことを確認する：

・政府のみでは、サイバー空間を十分に守ることはできない。重要インフラの防御は官民共同の責任である。

・政府はセキュリティに関する意識を向上させ、人々を教育し、脆弱性を発見かつ修正し、情報を交換し、そして復旧作業の計画をたてるために利用できる官民連携を促進するべきである。

・政府は、サイバーセキュリティプログラムの効率的な管理および監督を実行するために、包括的かつ省庁横断的な形で国家のサイバーセキュリティ政策や計画を策定し、調整することの可能な中央の組織を特定し、それに権限を付与するべきである。

・政府は、APEC、G8、OECD といった適切な多国間の枠組みの中で活動し、それらの枠組みで採択されたサイバーセキュリティやサイバー犯罪に関する勧告や行動計画を実施することが望まれる。

・政府は、適当と判断されるあらゆる手法でもって、サイバー事件に関する警告、脆弱性の情報、事故分析、そして修復に関する情報交換をするための監視･警告を行う事業体とメカニズムを設立するべきである。

・政府は、民間によるサイバーセキュリティ措置の進展を促すために、官民連携を促進する措置をとるべきである。

調整や民間との連携を行うためにそれぞれの政府内の中心的な機関を強調することを含め、米国と日本はサイバーセキュリティについて国家的なアプローチの重要性を確認する。更に、米国と日本は、サイバー犯罪条約を国際的に採択することを含む、サイバーセキュリティに関する多国間協力の重要性についても確認する。

日本においては、サイバー攻撃への対応策をつくり、電子政府を防御するために、内閣官房の情報セキュリティ対策推進室が設けられた。日本政府のサイバーセキュリティへの取組みの中で、情報セキュリティ対策推進室が先導的な調整役であり、その中心であることを日本政府は認める。日本政府が e-Japan 戦略 II で位置づけているように、代替の情報システム運用の確保、運用状況のフルタイム監視、緊急事態に対応するシステムづくり及び情報システムのセキュリティに関する情報の収集･共有により、サイバーセキュリティに関連する政府機関の間で協力を強固なものにしていくことが非常に重要である。それゆえ、情報セキュリティ対策推進室は、情報技術に関するセキュリティについての調整された政策立案における各省への助言、県等の地方政府との協調及び公的部門と私的部門の連携の構築等様々な活動を担当する。

米国国土安全保障省国家サイバー安全保障課は、他の様々な業務とともに、重要インフラや主要な

資源の脆弱性を減らすことを目的とした米国政府のサイバーセキュリティに係る取組みの中心となるとともに、民間部門や州／地方政府との連携を含むこのような取組みについて、米国内の関連省庁と調整する。国土安全保障省は、また、国際的問題については米国の外交政策を主導する国務省と緊密に協調する。司法省と連邦捜査局はサイバー犯罪を調査し訴追する国家的な取組みを主導する。大統領府の国家安全保障協議会は、重要な物理的及びサイバー上の主要なインフラ及び資産を含む国土を守ることを目的とした連邦政府機関や執行機関における国土安全保障に関する政策の調整を確保する。（以上）

英米、米韓は其々共同サイバー演習を実施しているが、日本では未だこうした試みが実現されていない。こうした共同作戦が強大なテロ集団に対抗する戦術であり、テロリストに対する予防的インパクトとにもなる。国際的演習も考えねばならないであろうが、先ずは国内における「経済安全保障」を趣旨とする官民共同のサイバーテロ演習が望ましい。

.

補遺

Appendix A

ソーシャルエンジニアリング

悪意のあるハッカーや外部攻撃者は、不正行為を成功させるために様々な方法を駆使している。人間を介したソーシャルエンジニアリングもその一つである。彼らはコンピュータシステムの情報だけでなく、社内の機密情報や個人情報など、一般に入手困難な内部の重要情報を盗み出す方法を常に模索している。セキュリティ対策が不十分である場合や組織構造に矛盾がある場合の脆弱性に加えて、実際には人間の行動や心理が悪用されて侵入されてしまう場合も多いのである。

ソーシャルエンジニアリングは、アクセスするシステムに関係なく、情報セキュリティにおいて最も脆弱な人間のミスや弱さを利用する手法であり、ソフトウェアやハードウェアに対して厳重なセキュリティ対策を施しても、この種の攻撃を防御することはできない。つまり、究極のセキュリティとは人間に対するセキュリティである。人間を騙すことができれば、侵入者はいとも簡単に防衛ゲートをかいくぐり、システムに侵入できてしまうのである。

特に重要インフラ企業においては、緊急対応時の迅速な行動が求められることから、社内のセキュリティポリシーを含む規範範囲が曖昧のまま業務しているケースが多い。NSA による極秘のサイバー演習「Eligible Receiver」において、内部者の成りすましを装った攻撃チームが社員からパスワードを入手してシステムへのアクセスに成功した事例があるため、ここでは特にソーシャルエンジニアリングについて項目を割いた。

ソーシャルエンジニアリングの定義

ソーシャルエンジニアリングとは、人間および信用するという人間の傾向を操作して組織のセキュリティ防御を侵害して攻撃する「技術」を指す。ソーシャルエンジニアリングの目的は、テクニカル・ハッカーの攻撃と同じである。攻撃はテクニカルではなく、ソーシャルスキルを利用して人的交流を通じて行われる。

ソーシャルエンジニアリングの分類

ソーシャルエンジニアリグは、大きく2つのカテゴリーに分類することができる。1つはコンピュータや技術を利用する手法であり、もう1つは人間を利用する手法である。技術を利用した手法では、「本物」のコンピュータシステムにアクセスしているとユーザーに信じ込ませ、ユーザーの機密情報を取得する方法がある。最近PayPal社のメールを装う「フィッシング」攻撃のように、例えば画面にポップアップウィンドウを表示し、アプリケーションに問題が生じたために再度認証を行う必要があるとユーザーに通知する。これにより、ユーザーにIDとパスワードを再入力させて、その情報を技術的に盗み出す。ポップアップウィンドウを作成したハッカーは、入力されたIDとパスワードを悪用し、そのユーザーの成りすまし

としてネットワークやコンピュータシステムに不正アクセスする。

人間を利用した手法とは、詐欺行為である。この手法では、対象者の無知を利用する場合や人間が本来持つ親切心や良心を悪用する。例えば、権限を持った人間に成りすまし、ヘルプデスクに電話をしてシニアマネージャーと名乗り、パスワードを忘れたのでリセットしたいと伝える。ヘルプデスクの担当者はパスワードをリセットし、電話の相手に新しいパスワードを伝える。これにより、攻撃者はマネージャの権限で人事制御システムにアクセスし、社員の社会保障番号や機密情報を入手することができる。攻撃者はネットワークに対するアクセス権を所有しているので、ネットワーク自体に大きな被害を与えることも可能である。

ソーシャルエンジニアリングの影響

セキュリティの専門家の間では、セキュリティ侵害の発生場所や実行者に関する見方は一致している。一般には外部のハッカーが侵入を行っているという印象が強いが、専門家らは侵入の多くが悪意のある内部の人間か、あるいは社内システムにアクセス権を持つ部外者によるものと考えている。FBIの調査によると、攻撃全体の80%はそのような権限のあるユーザーによって起こされている。

多くの場合、権限のある個人の行動を疑いの目で見ることはあまりない。誠実な人物の多くは他人も自分と同じように良心を持っていると考えている。侵入者は、このような人間の心理を逆手にとって、安心感を与え、警戒心を緩めさせる。1980年代および1990年代において悪名高いハッカーのKevin Mitnickは、BBC News Onlineとのインタビューで以下のように述べている。

■企業のセキュリティにとって最大の脅威はコンピュータウイルスではなく、重要なプログラムに存在するセキュリティホールでもなく、適切に構成されていないファイアウォールでもない。最大の脅威はユーザー自身である。
■個人的な経験から言うと、テクノロジーを悪用するよりも人間を騙すほうが簡単である。組織のほとんどが人的要因を軽視している。
■仮にわずかな知識しか持たないハッカーでも、その企業の社員になりすますことは可能であり、別の社員から無意識のうちに多くの貴重な情報を引き出すこともできる。

ソーシャルエンジニアリング手法

直接的な手法

ソーシャルエンジニアリングの一般的かつ直接的な手法としては、例えば仲の悪い社員の不慮の事故を悪用し、自分が仕事を引き継ぐとしてその社員のアクセス権を教えてもらう。その社員が復帰する前に同人のシステム権限を好きなように操作してしまう。

また、セキュリティ侵害の直接的な方法として尾行がある。悪意のある外部者が事務所の鍵を忘れ

た社員の振りをして、鍵を使って建物に入る別の社員の後に続けて建物に入る。尾行に気付かないかもしれないし、仮に気付かれたとしても、通常は後ろを振り返って尾行を止めるように言われることはない。建物への物理的な侵入に成功したことで、攻撃の第 1 段階を達成したことになる。

ダンプスター・ダイビング

ジャンクメールや通常の書類をシュレッダーにかけずに捨てる行為には、多くの危険性がある。例えば個人を特定できる情報やクレジットカード情報がジャンクメールに含まれている場合には、仮に断片的な情報であっても脅威となる。「ダンプスター・ダイバー」と呼ばれる人々は、そのような情報から個人情報を盗み出そうとする。

例えばゴミ箱を漁って会社の電話帳や組織図を入手することにより、社員の電話番号や住所を調べることができる。特に管理職クラスの情報を入手し、その社員に成りすまして不正な行為を行うことができる。また、職務規定や手順書を入手すれば、社内の規定や業務手順について知ることができる。これにより、対象者に自分は内部の人間だと信じさせることができる。カレンダーも重要な情報源である。ハッカーはカレンダーに記入された会議や休暇の予定を参考にして筋書きを立てて、例えば出張の役員を装って新入社員や警戒心の薄い秘書に急用の電話をして重要情報を引き出すことができる。

スパイ行為と盗聴

熟練したスパイであれば、背後から指の動きを観察するだけでユーザーのIDとパスワードを盗み出すことはたやすい。ヘルプデスクの担当者がユーザーにパスワードを伝えるときに電話を使用する規則になっている場合、ハッカーはその電話を盗聴してパスワードを盗み出すこともある。コンピュータに不慣れなユーザーはIDやパスワードをメモに書き残す傾向があるため、簡単に情報を盗み出すことが可能である。

技術的な専門家

侵入者がネットワークの問題を解決するサポート技術者に成りすまし、問題を解決するためにワークステーションにアクセスさせてほしいとユーザーに要求することもある。警戒心のないユーザー（新入社員など）は技術的な知識がない場合、何の質問もせずに偽の技術者にコンピュータを預けるかパスワードを教えるなど、社内のネットワークの問題を解決するために協力する姿勢を示す。

サポートスタッフ

警備や清掃員がネットワークに侵入するということは、誰も想像していない。しかし、清掃道具を持った作業服の男が仕事場に入り、ユーザーの机を掃除するふりをして、実は貴重な情報を取得しようと辺りを探索することもあり得る。このような場合、メモ書きされたパスワードや鍵を掛け忘れた機密ファイルなどがコピーの対象として狙われるほか、例えばその机からそのユーザーに成りすまして電話をかけることも考えられる。侵入者が電話の修理屋になりすます場合もある。修理屋の格好で電話に近

づき、機械の操作や回線の修理をするふりをして、実は保護されていない貴重な情報を職場から盗み出そうとするのである。

成りすまし

攻撃者は企業のコンピュータヘルプデスクに電話をかけ、内部者を装ってシステムへのアクセスに問題が生じたと嘘をつく場合がある。大至急でアクセスする必要があるので、パスワードを早急にリセットした上で新しいパスワードを教えてほしい、と電話で伝える。他のソーシャルエンジニアリングを用いて内部情報を入手している場合、さらに詐欺の信頼性を高めることができる。

トロイの木馬

攻撃者は無害のように見える電子メールを任意の受信者に送ることで、トロイの木馬型の攻撃を実行することができる。例えば、警戒心のない被害者がそのメールを開いてウイルスやワームに感染し、社内ネットワーク全体にも拡散させてしまう。I Love Youウイルスや、Anna Kournikovaワームが、その例である。

同様の方法でユーザーを攻撃するものとして、チェーンメールがある。このメールは、受信者が他の多くの人に転送すれば幸せが訪れ、そうしなければ不幸な結果が訪れるという内容である。このメールは、幸運をつかむ方法として害があるようには思われないので、ユーザーは要求された通りにする場合が多い。しかし、結果としてネットワークに過度の負荷がかかり、ネットワークが停止することになる。

ポップアップウィンドウ

不正なプログラムを利用してポップアップウィンドウを表示させることもできる。例えば、「ネットワークの問題によりアプリケーションの接続が停止したため、セッションを続行するにはIDとパスワードを再び入力する必要がある」という内容をユーザーに表示する。警戒心のないユーザーは作業を続行したいので、要求された通り入力操作を行う。前述した「フィッシング」詐欺の一種でもある。

ソーシャルエンジニアリングで攻撃する脆弱性

ソーシャルエンジニアリングは全て、人間の自然な性質を利用している。ソーシャルエンジニアリングの手法で利用される人間の性質は次の通りである。

・信頼（直接的な手法、技術的な専門家）
・親切心（直接的な手法、技術的な専門家、成りすまし）
・無料で何かを得ようとする心（トロイの木馬、チェーンメール）
・好奇心（トロイの木馬、覚えのない送信者からの添付ファイルを開く）
・未知の物への恐怖心、何かを失うことへの恐怖心（ポップアップウィンドウ）
・無知（ダンプスター・ダイビング、直接的な手法）

・無警戒（ダンプスター・ダイビング、スパイ活動及び盗聴）

被害対策

・詳細なセキュリティポリシーの施行と徹底
・セキュリティポリシーに関する持続的な教育
・ソーシャルエンジニアリングの脅威や被害に関する意識の向上
・ポリシーの実施と監査
・運営規則の明確化
・脆弱性を軽減する作業手順
・不正侵入の回避や防止のための物理的な技術ソリューション（生体認証システムなど）
・保険を利用した被害の軽減

セキュリティポリシー

詳細なセキュリティポリシーの策定と施行、それに関連する基準やガイドラインの適用などにより、効果的なセキュリティ戦略の基礎が整う。ポリシーでは適用される分野ごとに、素人にもわかりやすい言葉でその目的と内容を明記しなければならない。それぞれのポリシーを作成すると同時に、それに従って基準とガイドラインを作成する必要がある。ポリシーを文章化した後に、組織の全ての人間が簡単にそのポリシーに目を通せるように普及させる必要がある。企業のイントラネットにポリシーを公開するか、もしくはイントラネットの他の主要ページにポリシーページへのリンクを張ることが望ましい。

教育

ポリシーを有効利用するには、教育が日常的な課題となる。毎年全ての社員にポリシーを確認させ、訂正箇所があればそれを習熟させる会社もある。新入社員や外部者には、配属後できるだけ早く教育を受けさせる必要がある。

脅威と危険行動に関する知識の向上

情報詐欺師が使用する手口と狙われる行動についての知識を向上させることは防衛戦略の重要な一部であり、詐欺の損害について社員を教育することも必要不可欠である。セキュリティの専門家でない社員に対して意識の向上を図る最良の方法は、実体験に基づいた例を教えることである。内部情報や社員の怠慢や無知が原因で、企業に侵入されたケースなどを説明するのが有益である。

ポリシーの遵守状況の確認

ポリシーを作成して教育を行っても、実際に従わなければ意味がないため、企業全体でポリシーの遵守状況を監視する必要がある。例えば、あるプロジェクトが品質保証の段階に至った際、セキュリテ

ィポリシーの順守査定も同時に行うべきである。監査手順は段階別に作成する必要がある。入り口などのアクセスポイントは毎日監視する。これにより、保護された施設への入出館規則を社員が順守しているか確認することができる。職場では抜き打ち調査を行い、機密文書が鍵の掛けられた保管庫で保護されているかどうかを確認する。ワークステーションには鍵を掛け、パスワード保護付きのスクリーンセーバーを使用すべきである。

ID管理

企業では、各社員に固有のIDを割り当てるのが一般的である。IDは企業の個人を特定するだけでなく、全てのコンピュータシステムへのアクセスに使用されることが多い。しかし、すべての特定プロセスで同一のIDを使用することは危険である。例えば、外部の侵入者が社員IDを発見した場合、その社員のアクセス権が与えられているネットワークやコンピュータプリケーションにアクセスできる可能性がかなり高くなる。個人IDとコンピュータシステムに使用されるIDを区別することで、作業量は多少増えることになるがリスクを軽減することができる。

運用手順

標準的な運用手順を作成する場合には、要求を認証する前に相互に相手を確認する方法や電話の場合は必ずコールバックを行うよう定める必要がある。これにより、ハッカーは他人に成りすますことが難しくなる。

保険による保護

最近では、セキュリティ攻撃に対して保険を掛けることができる。保険会社の多くは、企業が攻撃を回避するために適切なポリシーや運用手順を策定し、施行しているかどうかを査定する。保険会社は、攻撃回避にどのような製品を使用しているかではなく、策定したポリシーがどの程度徹底されているかを重要視している。例えば、次のような項目を評価する。

・内部監査ポリシー
・パスワードポリシー
・採用基準　(身元調査に関するポリシー)
・従業員及び協力会社の要員に対するセキュリティの意識付けや研修プログラム
・ベンダーなどとの契約

結論

ソーシャルエンジニアリングによる攻撃を回避できなかった場合、サイバー攻撃と同等の甚大な被害を被る可能性が高い。そのため、優れた情報セキュリティ戦略は企業戦略全体において重要な要素となる。

セキュリティ戦略を企業全体に浸透させて徹底させることにより、ソーシャルエンジニアリングによる攻撃を回避することができる。詳細なセキュリティポリシーを作成し、公開するだけでなく、研修プログラムなどを通じてセキュリティに対する意識を向上させることが重要である。また、監査プログラムを策定し、ポリシーの遵守状況を監視する必要もある。不審者の侵入を物理的に阻止するためのセキュリティ装置の導入だけでなく、セキュリティ攻撃に対する保険を掛けることも必要である。

Appendix B

最も脆弱なのは人間――ソーシャルエンジニアリング

ソーシャルエンジニアリングは、比較的低コストで実行でき、しかも効果的である。単純な質問で多くの大規模なセキュリティ・システムを危険にさらすことができる。人が単に尋ねられた時どの情報を喜んで提供するかは驚きである。相手が断ることもあり得るが、何かを頼むことは簡単に実行でき、しかも無料なのでソーシャルエンジニアリングの基礎となっている。

しかしながら、ソーシャルエンジニアリングが単純であるとは限らない。ソーシャルエンジニアリングは、他のテクニカル・ハッカーの攻撃と同類のレベルの準備を要求する。ソーシャルエンジニアリングがそれほど効果的で簡単なのは、情報セキュリティ界で最も弱いリンク（部分）をターゲットにしているからである。つまり人間である。

どのシステムであっても最もセキュリティが弱いのはユーザーである。全ての情報システムが人間に依存していることが認識されているように、ユーザーは普遍的脆弱性のある「独立したプラットフォーム、ソフトウェア、ネットワーク、設備経年数」である。下記の情報は、人間がソーシャルエンジニアリングの攻撃に対して脆弱であるための心理学的および行動の特性の抜粋である。ソーシャルエンジニアリングの攻撃者は、ターゲットが要求に従うようにこれらの特性につけ込むのである。

説得 【Persuasion】

説得は、全社会で使用される芸術と科学である。広告とマーケティング業界は、特定の反応を導くためにデザインされたキャンペーンを生み出す説得の専門家である。このような産業のように、「人間は、注意深い巧みな操作によって搾取できる特定の行動を持つ傾向がある」ことをハッカーもまた発見している。ソーシャルエンジニアリング攻撃を用いたハッカーは、説得を通じてターゲットに情報を明らかにさせる能力に優れている。

役に立つ傾向 【Tendency to be helpful】

人間は、役に立ち、礼儀を守る傾向がある。両手が塞がっている人のために、エレベーターのボタンを押したり、ドアを開けたりするのがその一例である。箱いっぱいの道具と備品を抱えた保守技術者を装った人は、しばしば、ドアを開けたままにしてもらえるだろう。適切な服を着た専門家は、アクセスキーを別のコートに入れたままだと主張し、誰かにエレベーター・アクセスを頼むかもしれない。これらの共通の礼儀は、物質的セキュリティの裏をかき、攻撃者にオフィスでの自由な支配を与える。

責任の分散 【Diffusion of responsibility】

責任の分散とは、個人が自分たちの行動に単独で責任を負わないと信じている概念である。ソーシャルエンジニアリングの攻撃者は、個人が全面的な責任を負う必要はないという錯覚を巧みに作り出す。

これは、上司がそういった要求を許可したと伝える方法や、または他のターゲットに馴染みのある人も関係しているとターゲットに知らせることによっていとも簡単に成功する。攻撃者はその時、より簡単にターゲットから情報を聞き出すことができるのである。

迎合 【Ingratiation】

迎合とは、従順を増していく人間の行動パターンである。迎合は影響力を得るために、賞賛、お世辞、または友好的かつ有益な態度を示し、2つの方法で機能する。しばしば攻撃者は、迎合でターゲットに取り入り、ゆっくりと要求のための根回をして信頼関係を築く。信頼関係の目的は、ターゲットをもっと要求に応じるような立場に置くことである。

迎合は、ターゲットが攻撃者に取り入りたいと考えるような環境を攻撃者が作り出す時にも発生する。例えば、攻撃者は有名な人の名前を出して、将来ターゲットを援助できるという錯覚を作り出すことも可能である。この筋書きによって、ターゲットは有利な銀行に頭金を支払ったと信じているので、攻撃者の要求はさらに認められやすい。

道徳上の義務 【Moral duty】

真偽の概念である善と悪は、しばしば早い段階から全ての人間に教え込まれている。これらの概念は、人のモラルを形成する役割を果たし、言動や行動を導く。道徳上の義務は、自分の確信と信念に基づいて行動するように自分たちを強いていると感じる概念である。ソーシャルエンジニアリングの攻撃者は、ターゲットが自分たちの道徳上の義務に従って要求に応じているという状況を作り出すことによってこれを逆に利用している。

攻撃者は、ターゲットが要求に従わないことは結局罪になるという筋書きを作り出すことで利用することも可能である。この例としては、ターゲットが要求に応じない場合は、要求者（攻撃者）が職を失うかもしれないとターゲットに信じ込ませる場合などがあげられる。

他の特性 【Other traits】

上記で述べた特性と行動は、ほんの一例にすぎない。人間は、積極的な社会環境を確保する多くの他の特性や行動を持つ自然社会性の高い生き物である。

他の特性は下記に記す：

- 役立ちたい願望 – 私達は、いざという時に同様の援助をありがたく思うため、人はもともと他人を手助けする傾向がある
- 自分たちと他人のために不愉快な出来事を回避する願望 – 人は同情的で他人に苦痛や不快感を与えたがらない
- 仕事において有能でありたい願望 – 特に自分の専門分野では、だれからも能力がないと見られたくない

- 他人を信じる願望（他の方法で証明されない限り他人が言ったことを真実であると受け入れる傾向） – 人は、他人に対して「疑わしきは罰せず」の傾向がある
- 動機とキャリアを向上させる願望 – 人は、日和見主義で可能な場合および可能な時、自ら努力する。
- 賞嘆する人または好ましい人に対して魅力的でありたい願望 – 人は一般に受け入れられることを望んでおり、尊敬する人に対してはなおさらである。私達は、従順によってやがては受け入れられると信じている。
- 対応する人が尊敬すべき人だと信じたい願望 – ここでも他人に対して「疑わしきは罰せず」をあげる
- チームメンバーであると認識されたい願望 – チームワークは、多くの組織で共通の本質的価値観である。これは広く期待され、社会型人間でないとキャリアの妨げとなる影響を及ぼすことさえあるかもしれない

これらの特性は全て、ソーシャルエンジニアリングからの攻撃を極めて受けやすくしてしまう。しかし、どんな脆弱性でも、組織がこれらの脆弱性を軽減できる対応策と措置がある。

脅威のベクトル 【Threat vectors】

ソーシャルエンジニアリングの攻撃は、あらゆる方向からやって来る可能性がある。これらの様々な攻撃ポイントは、脅威のベクトルとして知られている。情報セキュリティの専門家がソーシャルエンジニアリング攻撃の適切な対応策を開発する前に、脅威のベクトルと攻撃者が、いかに正確に、人と人とのコミュニケーション手段を組織の機密情報とシステムに変えるのかを理解することは重要である。

ダンプスター・ダイビング 【Dumpster diving】

ダンプスター・ダイビングは、有益な情報を探すために会社のごみ箱の中を捜す方法である。ダンプスター・ダイビング自体は攻撃性の高い行為ではないが、会社の重要な情報を攻撃者に提供するであろう。

この情報は、フットプリンティング・プロセスとして使用される。*Hacking Exposed* は、フットプリンティングを「ターゲットの情報を収集する芸術」と定義している。一方で次のように指摘している。「フットプリンティングは実在のセキュリティ態勢を決定するのに最も骨の折れる仕事である。これが最も重要な作業の1つである。」ちょうどテクニカル攻撃のように、成功のキャンペーンの秘訣は、実際の実行よりも準備にある。ダンプスター・ダイビングは、下記のアイテム全てから生じる可能性がある。

会社の電話リストまたは電話帳	会社のポリシー・マニュアル
組織図	システム・マニュアル
メモ	ソースコードのプリントアウト

会議、イベント、休暇のカレンダー	機密データのプリントアウト（ログイン名やパスワードを含む）
会社のレターヘッド	旧式のハードウェア、ディスク、テープ

これらのアイテムで、ターゲットとなる組織についての豊富な情報が明らかになる。これらは、なりすますことのできる本物の名前や個人の肩書きを提供してくれる。会社のレターヘッドは、正式の要求を偽造するために使用される。システム・マニュアルで、攻撃者はどのシステムが実行されているかわかるため、その後の要求をする時に具体的にそれらを参照することができる。

電話 【Phone】

最も一般的なソーシャルエンジニアリングの脅威のベクトルは電話である。電話は、社会が使用する人と人のコミュニケーションとして広く受け入れられている方法である。ビジネスは、しばしば電話でやりとりする。人は、電話で要求を行い、また要求を承諾することに慣れてきている。電話でのコミュニケーションがあまりにも一般的なので、どの要求が正当なもので、どれがソーシャルエンジニアリング攻撃の可能性があるか、ターゲットが判断することが困難になっている。

電話でのソーシャルエンジニアリング攻撃は、しばしば成りすましを含む。通話主はうまく成りすまして、攻撃者に必要な情報を提供する厳密なフットプリンティングを行う。機密である必要はないが、組織の経営構造（重要人物の具体的な名前と肩書きのある）、現在および未決のプロジェクト、他の詳細事項などの情報は、攻撃者が正当な要求をしているとターゲットに確信させるのに役に立つだろう。

導入で論じた筋書きに加え、別の例として、攻撃者がヘルプデスクの技術者を装ってターゲットに電話をすることがある。技術スタッフは、いくつかのアップグレードを行っており、プロセスを完了するためにはターゲットのユーザーネームとパスワードが必要であるとターゲットに告げる。何も気づかないユーザーがその要求に応じる可能性は高い。

電子メール 【Email】

電子メールは、攻撃者が利用できる人と人のコミュニケーションのもう1つの手段である。 ほとんどの電子メールアプリケーションでは、電子メールでユーザーが送信と返信のフィールドを変えることが可能である。これらの設定を操作して、正当な要求をする誰かに成りすますことができる。

電子メールの添付ファイルもまた主な関心事である。電子メールは、通常気づかない内にファイアウォールを通過するので、破壊的プログラムがシステムへ自由に入れる。特に、電子メールがターゲットの認識する人物から送られた場合なら、潜在的に悪影響があるとは少しも考えず、無分別に添付ファイルを開き、その時にユーザーはこれらのプログラムを放つ。これらの添付ファイルは、ウイルス、ワーム、トロイの木馬の可能性があり、しばしばユーザーにアプリケーションを実行するよう誘発する方法で見せかける。添付ファイルがどのタイプであってもシステムに大損害を与えることが可能である。

IRC/インスタント・メッセージ 【IRC/Instant messaging】

インスタント・メッセージ (IM)は急成長した。ビジネスでは、ビジネス・コミュニケーション (ワークグループのコラボレーション・ツールとして) のさらにもう1つの方法として IM をゆっくりと受け入れている。こういったツールがオフィスでますます普及するにつれて、情報セキュリティの専門家は、潜在的な脆弱性を知る必要がある。

Carnegie Mellon 大学の The Computer Emergency Response Team (CERT)は、インターネット・リレー・チャット (IRC) と IM を経由してのソーシャルエンジニアリング攻撃の詳しい事件の情報を最近刊行した。この情報の中で CERT は、「疑いを持たないユーザーが悪質なソフトウェアをダウンロードもしくは実行してしまう」攻撃を警告している。悪質なソフトウェアは、ダウンロード速度の向上やアンチウイルスのかいくぐりなど洗練化しており、またはポルノグラフィーを提供するアプリケーションとして見せかけている場合もある。CERT の情報が指摘しているように、この試みの成功はユーザーがプログラムをダウンロードして実行するかしないかに完全に依存しているので、これは古典的なソーシャルエンジニアリング攻撃である。

対応策 【Countermeasures】

上記で概要を述べた様々なソーシャルエンジニアリング攻撃の一方で、組織がこういったタイプの攻撃の検知と回避を実行できる多くの対応策がある。下記に、人的要因を軽減する対応策を論じる。

物理的セキュリティ 【Physical security】

物理的セキュリティは、組織が直面する可能性のある脅威の種類に関係なく、実行しなければならない対応策の1つである。物質的セキュリティは、関係者のみ組織の構内への出入りを許可することから始める。多くの組織には、誰がビルを出入りしたか監視するセキュリティ・ガードがある。さらに、会社には、訪問者のアシストを担当する受付係がいる。

セキュリティポリシー 【Security policies】

明確なセキュリティポリシーは、ソーシャルエンジニアリングの攻撃に対する防御において、重要な要素である。ポリシーは、「従業員の責任を排除し、ハッカーの要求に関して判断を決定できる。その行為がポリシーによって禁じられている場合、従業員はハッカーのリクエストを拒絶しなければならない」下記に Gartner Group が奨励するいくつかのセキュリティの方法をあげる。

- パスワードの変更を一切排除する手順を確立する。システム管理者は、決してユーザーにパスワードを聞いてはならず、システム上で全てのパスワードを見ることさえもできない。
- 確固たるパスワードを奨励し、攻撃者が簡単に識別できるパスワードや認証質問の使用を避ける。

- 最近退社した従業員の電子メールとシステム･アカウントを削除する。長期休暇の従業員に対してもこれらのアカウントを削除する。

セキュリティポリシーは、どの操作が許可され、また制限されるかの行為の許容ルールと厳格なアウトラインを従業員に提供しなければならない。それらは、一般的または特定であるが、常に明確で簡単に理解できる必要がある。さらに、ポリシーでは従わない場合の結果などの強制措置も列挙しなければならない。

意識向上のトレーニング 【Awareness training】

セキュリティポリシーに加え、ソーシャルエンジニアリングを防御する他の重要な要素は、十分に教育された従業員である。セキュリティポリシーは、従業員がポリシーに精通している場合のみ有効である。意識向上のトレーニングは、セキュリティポリシーの見直し、および、それぞれの指令に隠された目的と動機付けを含んでいる。従業員は、リスクとポリシーが侵害された場合、何が問題となるかを理解する必要がある。

効果的な意志向上プログラムは、セキュリティの脅威に対して従業員を教育するだけではなく、彼らをセキュリティ･プロセスの一部にする計画である。従業員には、組織の安全を保証するにおいて、特定の役割と責任を与えるべきである。Gartner は次のように述べている。「ユーザーがこれらの問題を理解すれば、さらにそれらに従い、不審な行動に気づくであろう。ソーシャルエンジニアリング攻撃に対する単独で最強の防御は、教育された従業員である。」上記で論じたように、ソーシャルエンジニアリングの脅威のベクトルは 至る所にある; 従業員は、それらが何であるのか知る必要があり、またそれらを安全化するだけではなく見つけ出すことができる必要がある。

インシデント･レスポンス 【Incident Response】

組織は、教育されたユーザーが疑わしい行動を報告できるような効果的なインシデント･レスポンス･プロトコルを持つ必要がある。ユーザーの意識向上トレーニングは、ソーシャルエンジニアリング攻撃を見つける方法で従業員を教育した。今回は、これらの事件を報告する手段を定義する必要がある。これは従業員に権限を与え、彼らをセキュリティ･プロセスの一部にするものである。

さらに重要なことは、組織は事件に取り組んでいることを従業員に知らせるフィードバック･コントロールをする必要がある。事件の報告は尊重して扱い、後に続く必要がある。そうでなければ、「従業員は、疑わしいソーシャルエンジニアリング攻撃に対する注意または報告することに意欲を減退させるであろう。」

アクセス･コントロール 【Access controls】

アクセス･コントロールは、最小の特権の原則を実施する。最小の特権の原則は、ユーザーまたはシス

テムに 、そのタスクを完成するために要求される必要なアクセスのみを行うことを求める。アクセス・コントロールは、初心者が引き起こす可能性のある損害を制限する。例えば、ソーシャルエンジニアリングの攻撃をより受けやすい受付係は、機密ファイルを電子メールで送るように依頼されるかもしれない。しかしながら、適切なコントロールが存在する場合、その特権は受付係の任務には必要ではないので、受付係はそれらのファイルにアクセスすることはできないはずである。

アクセス・コントロールは、さらに、ユーザーがアカウントを作成、修正、削除するのを防ぐだけでなく、悪質なソフトウェアをダウンロードやインストールするのを防ぐこともできる。ターゲットがソーシャルエンジニアリング攻撃によって危険にさらされた場合、アクセス・コントロールは、攻撃者が原因で起こる損害の量を制限することができる。もう一度述べるが、攻撃者が受付係のログインやパスワードを危険にさらした場合、攻撃者は、受付係の 限られた特権によって制限される。

アンチウイルス 【Anti-virus】

アンチウイルスは、多くの組織が実施する防御の共通レイヤーである。この防御のレイヤーは、ユーザーにファイルをダウンロードやインストール（例えば、電子メール、IRC,インスタントメッセージ・アタック）を要求するソーシャルエンジニアリング攻撃に対して優れた対応策となる。アンチウイルスのソフトウェアは、悪質なソフトウェアの脅威のサインを認識し、インストールされるのを防ぐものでなければならない。もちろん、単にその定義ファイルと同質であるから、アンチウイルスのソフトウェアのアップグレードもまた、課題の対応策の一部である。

結論 【Conclusion】

昨年、企業はセキュリティに数百万ドルを費やした。ほとんどの額が、ファイアウォール、境界ルータ、侵入検知システム等のテクニカル・ソリューションに費やされた。多くの企業は、情報セキュリティ問題の最善の対処法はお金をかけることだと信じている。防御は、攻撃者を阻止するために構築したハードウェアやソフトウェアの数に直接関連する。しかしながら、経験豊かなセキュリティの専門家は、これはそのケースに当てはまらないことを知っている。

テクニカル・ソリューションが情報セキュリティ・チェーンにおいて重要な要素である一方で、ソーシャルエンジニアリング攻撃は、最も弱いリンクである人間を攻撃する。人間は、すべての情報システムと接触するので、結局は、広範囲に渡る脆弱性となる。他の脆弱性と同様に、最善の解決法は徹底的な防御を要求する。これらのレイヤーは、物理的なレベルから始まり、マネージメント・レイヤー（上層部のマネージメント・バイ・イン、セキュリティポリシー、ユーザー意識の向上、インシデント・レスポンス）だけでなく、テクニカル・レイヤー（アクセス・コントロール、アンチウイルス）を含む。大半の情報セキュリティ問題と同様に、解決策は、マネージメントに焦点を当てている。組織は、単なるテクニカルな観点からだけでなく人的な観点から自分たちの適切な安全のために必要な時間（お金）をかけさえすれば、セキュリティ態勢を強化できる。

ヒアリング先

・Michael Vatis	Executive Director	MARKLE FOUNDATION
・Martin N. Wybourne	Associate Dean	DARTMOUTH COLLEGE
・Andrew Cutts	Scenario Development	DARTMOUTH COLLEGE (ISTS)
・Brian J. Kelly		ERNST & YOUNG
・Lawrence F. Lederer	Principal Engineer	Westin Solutions
・Joseph Weiss	Executive Consultant	KEMA Inc
・Frank S. Lim	Director B-Development	KEMA Inc
・Wade P. Malcolm	President & CEO	EPRI
・Robert B. Schainker	Senior Tech Leader	EPRI
・Yvonne Wong	CFO	EPRI
・Burk Kalweit	Senior Manager	EPRI
・望月正夫	日本代表	EPRI ワールドワイド

その他

・著名ハッカー

・DHS

・IAIP

・IRIA

・FBI

・NIPC

・NSA

・米空軍

・その他政府機関担当者

参考文献

財団法人　電力中央研究所の各種報告書

「電力自由化が及ぼす電力通信網への影響と課題」

「広域イーサネット方式による電力用通信網の構成」

「広域イーサネット方式による電力用通信網の構成（その2）」

「電力用 DTM 統合通信網の基本設計」

「アクセス系ネットワークの技術動向と電力通信網への適用方法の検討」

「分散リアルタイムネットワークアーキテクチャの開発（その1）」

「分散リアルタイムネットワークアーキテクチャの開発（その2）」

「分散リアルタイムネットワークアーキテクチャの開発（その3）」

「分散リアルタイムネットワークアーキテクチャの開発（その4）」
「ネットワークレイヤ毎のセキュリティ分担方式」
「設備診断のための異常・予兆発見手法」
「テラヘルツ電磁波発生技術の動向と課題」

米国関連書籍

「Black Ice　the invisible threat of cyber-terrorism　Dan Verton」
「Hacking Exposed　third edition　Foundstone」

米シンクタンク資料

「Cyber Security of the Electric Power Industry」
「North America's Electric Infrastructure: IEEE Security & Privacy」
「The Blackout of 2003　view points from ICF Consulting」
「Electricity Sector Framework for the Future」
「Interviewing with An Intelligence Agency」
「Digital Pearl Harbor: defending your critical infrastructure」
「サイバー攻撃とサイバーテロ　Gartner」
「サイバーテロへの対処　Gartner」
「Emergency Incident Response」
「Microsoft Active Directory Connector and the Windows Web」
「A Day with the C&W Cyber Attack Team: Nimda Worm」
「Emergency Incident Response to Linux Server Infiltration」

米東海岸で起こった 8.14 停電資料

「北米大停電事故の中間報告をレビューする　電力中央研究所」
「ニューヨーク大停電危機にどう対処したか　未来政策研究所」

我が国に関する資料

「情報セキュリティ総合戦略　経済産業省」
「情報セキュリティの現状と動向　防衛調達基金整備協会」
「危機管理のノウハウ　PART 1　佐々淳行」
「危機管理のノウハウ　PART 2　佐々淳行」
「危機管理のノウハウ　PART 3　佐々淳行」
「超限戦　坂井臣之助（監修）」
「21 世紀の戦争　James Adams」
「ハッカージャパンマニアックス　ハッカージャパン編集部」
「インシデント・レスポンス　Kevin Mandia」
「情報テロ　江畑謙介」
「サイバーテロ　浜田和幸」
「グローバル・インテリジェンス・ファイル　落合信彦」

「2004 周波数帳　三才ブックス」
「原子力発電で本当に私たちが知りたい 120 の基礎知識　広瀬隆」
「情報通信白書　総務省」
「インターネット･セキュリティのしくみ　熊谷誠治」

Web 公開資料

「Computerworld security」
「washingtonpost.com」
「The Register」
「The Homeland Report」
「The New York Times」
「Wall Street Journal」
「Full-Disclosure digest」
「Infowar」
「SecurityFocus」
「SITE Institute」
「中央給電システム」
「東京電力ホームページ」
朝日新聞　http://www.asahi.com/
毎日新聞　http://www.mainichi.co.jp/
読売新聞　http://www.yomiuri.co.jp/
日本経済新聞　http://www.nikkei.co.jp/
共同通信　http://www.kyodo.co.jp/
ガーディアン　http://www.guardian.co.uk/
ニューズウイーク誌　http://www.nwj.ne.jp/
タイム誌　http://www.time.com/time/
ＣＮＮ　http://www.cnn.com/
ＢＢＣ　http://news.bbc.co.uk/
ＡＰ通信　http://www.apbroadcast.com/AP+Broadcast/default.htm
米国連邦　http://www..firstgov./
ニューヨーク州　http://www.state.ny.us/
ニューヨーク市　http://www.nyc.gov/portal/index.jsp?pageID=nyc_home
コン･エディソン社　http://www.conedison.com/
ＮＥＲＣ　http://www.ferc.gov/
ＮＹＩＳＯプレス　http://www.nyiso.com/

その他独自情報源