3．特集：サイバーセキュリティ対策

- 国家の重要インフラをいかにサイバー攻撃から守るか -

情報通信ユニット 清貞 智会、客員研究官 山田 肇

3.1 はじめに

2001年9月11日、米国において同時多発テロが起こり、米国のみならず世界中が混乱の渦に巻き込まれた。わずか数十名の実行犯によるテロ攻撃が、数千人におよぶ死傷者を出す大惨事を引き起こし、また、数日間にわたって都市機能を麻痺させたのである。

さらに、米国主導による報復攻撃が続いている現在、テロリストによる逆報復の脅威が高まっている。もし逆報復があるとすれば、どんな手段が用いられるのであろうか。また、政府はどのような対策を講じべきであろうか。

本稿ではサイバーテロに焦点を絞り、早くからサイバーセキュリティ政策を進めてきた米国の取り組みを紹介することで、わが国のサイバーセキュリティ政策立案の一助とする。

3.2 サイバー攻撃の脅威

3.2.1 逆報復は起こるのか？

10月11日、FBI(米連邦捜査局)は正式に、「数日以内に新たなテロが起こる疑いがある」との警告を発した("Immediate Release", FBI National Press Office)。また、Washington Postは10月5日付けで、「FBI、CIA(中央情報局)およびDIA(国防情報局)の担当者が、非公式に上下両院情報特別委員会の議員に対して、「米国が報復を行った場合、テロリストは100%逆報復する。」と報告した。」と伝えている("FBI, CIA warn Congress of more attacks as Blair details case against Bin Laden", Washington Post)。

3.2.2 サイバー攻撃による逆報復

もしテロリストが逆報復するとすれば、どんな手段が使われるか。テロリストのリソースが少ないことを推察すれば、逆報復はミサイルを使った武力攻撃でなく、少人数および低コストで実行できる生物・化学テロやサイバー攻撃である可能性が高い。

実際、米国では次々と炭そ菌患者が発見され、生物テロの脅威が高まっている。しかし、各地でテロに対する厳戒態勢が敷かれている現状を考慮すれば、遠隔地から実行できるサイバー攻撃も生物テロに劣らず非常に大きな脅威であると考えられる。現に、「親テロ派・反テロ派の支持者は、それぞれハッカーグループを幾つか立ち上げ、米国企業やイスラム諸国政府などのウェブサイトに対し、サイバー攻撃を始めている。」と、サイバーセキュリティ専門の情報機関であるiDEFENSE社は指摘している(iDEFENSE Report #105540, #105551)。

3.2.3 テロリストのサイバー攻撃能力

次にテロリストのサイバー攻撃能力について検討する。

報道では、「ビン・ラディン氏は、ステガノグラフィという技術を用いて極秘にテロ活動に関する指示を送っていた疑いが強い。」と言われている("Terror groups hide behind Web encryption", February 6, 2001, USA TODAY)。

ステガノグラフィとは、極秘のテキストや画像データを、インターネット上にあるテキスト、画像および音声ファイル等に埋め込んで送る技術である。ジョージメイソン大学のジョンソン博士は、ステガノグラフィを使ってデータを埋め込んだ画像と、埋め込む前の画像を同氏のウェブサイト(http://www.jjtc.com/stegdoc/sec313.html)上で対比しているが、目視では違いを判断することが困難である。通常、情報を極秘に送る場合には暗号技術が利用されることが多いが、情報が隠されていることが明示的な暗号に比べて、そこに情報が隠されていること自体が第三者に分かり難いステガノグラフィは秘匿性が高い。また、暗号はネットワーク上のデータトラフィック傍受システムに検知され易いが、ステガノグラフィだと検出される可能性は極めて低い。

また、前クリントン政権下でNSC(国家安全保障会議)のサイバーセキュリティ部門を統括していたヒュンカー氏は、「9月11日のテロ攻撃は周到に準備されたものであり、実行犯達は教養が高く、また豊富な資金を持っていたと推測できる。もし彼らがサイバー攻撃を行ったとしても、米国に大きな打撃を与えていた可能性が高い。」と指摘して

いる("U.S. Networks Run Big Risk of Cyber-strikes", Experts Assert, October 3, 2001, Mercury News)。

本章では①サイバー攻撃の脅威、②テロリストのサイバー攻撃能力について分析した。次章以降では、早くからサイバーセキュリティ政策を進めてきた米国に着目し、米国が同政策に取り組むようになった経緯、および同政策の概要等を紹介する。

3.3 米国におけるサイバーセキュリティ意識の高まり

IT の発展に伴い、国防、電気、天然ガス、電話、交通等の重要インフラがインターネット接続されるようになった。これは利便性を高める一方で、システムの脆弱性も高めている。こうした中、米国では、数年前から重要インフラへの不正侵入の試みが頻繁に検出され("Emerging Challenge: Security and Safety in Cyberspace", Ver. 14, No. 4, Winter 1995-1996, IEEE Technology and Society Magazine)、重要インフラへのサイバー攻撃が国家安全保障上の新たな脅威であるとの認識が高まっている。

3.3.1 サイバー攻撃を想定した演習

1996年3月23日、DOD(国防総省)のDARPA(国防高等研究計画局)が、重要インフラに対するサイバー攻撃によって引きおこされる様々な被害を想定した演習「The Day After ...」を行った("Strategic information warfare : a new face of war", Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, Rand Corporation)。同演習では、図表1に示すサイバー攻撃のシナリオが想定された。

図表1　想定されたサイバー攻撃

日時(米東部夏時間)	概要
5月11日夕方	NCC*がホワイトハウスへ、①「カリフォルニア州北部とオレゴン州の電話回線にトロイの木馬*が仕掛けられ、回線が不通になった。」、②「ワシントン州フォートルイスの軍事基地の基幹回線が DOS 攻撃を受け、通信システムが数時間、機能不全に陥った。」と報告。
5月11日深夜	カイロ(エジプト)の電力供給システムが故障し、90%の世帯が数時間にわたって停電。
5月13日4:00	サウジアラビア南東部の大規模石油精製施設にて制御システムが故障、爆発し、火災が発生。
5月14日18:12	メリーランド州で運行制御システムに埋め込まれた論理爆弾が爆発し、貨物列車と高速列車が衝突。メリーランド州警察は、「死者60名、負傷者120名。」と推定。
5月16日6:00	スコットランドヤードが英首相に、「英中央銀行の送金制御システムの3か所が故障。事態を重く見た銀行首脳部が送金サービスを停止。」と報告。
5月20日午前	米統合参謀本部の情報戦争計画部隊が「DOD のコンピューターの時分割実行制御プログラムに正体不明のコンピューターワームが蔓延している。」と発表。
5月20日12:10	ジョージア州の2大銀行の ATM システムがそれぞれ故障し、取り付け騒ぎが起こった。この結果、両銀行は ATM システムを閉鎖。
5月20日12:25	アトランタ地区の CNN ニュースセンターからの放送が12分間不通になった。
5月20日15:30	CNN が米国のサイバー攻撃に対する脆弱性をテーマにした特別番組を放映。ここでは、当日、全米でサイバー攻撃によって生じた、①ボストン-ニューヨーク-ワシントン DC をつなぐ特急列車の衝突事故、②北西部の電話回線麻痺、③アトランタの ATM システムの閉鎖、④原因不明の CNN 送受信装置の故障、等について報道。
5月20日夕方	全米ネットおよび地方ネットのイブニングニュースが、「陸軍および海軍の LAN や電話回線がサイバー攻撃されたため、湾岸地区における米軍の活動に支障をきたしている。」と報道。
5月22日19:44	シカゴのオヘア空港へ着陸寸前のエアバス340型コンチネンタル航空機の機長が、管制塔に、「翼制御機器が故障し、航空機を操縦できない。」と報告。
5月22日20:05	オヘア付近の地方警察が、「空港南方の住宅地に大型航空機が墜落。現在のところ、生存者はなし。」と発表。
5月22日夜	英国から「最新のエアバス330型および340型航空機のフライト制御プログラムの全てに精巧な論理爆弾が仕掛けられている。」との報告を受けた米国連邦航空局は、米国内にいるすべての最新型エアバス330機、340機に対して、「飛行中のものは即刻着陸し、エアバス340型航空機の墜落事故原因が明確になるまで飛行を禁じる。」と命令。

5月23日 12:57	サウジアラビアの公共回線交換網の制御プログラムがトラップドアにより改ざんされ、機能不全に陥った。
5月23日 16:10	統合参謀本部長はDOD長官へ、「米国や欧州の大部分の軍事施設において、全面的な情報戦争が進行中である。現在のところ、犯人は不明。」と報告。
5月23日 19:00	湾岸地域において複数のレーダー搭載偵察機がコンピューターワームに感染。
5月24日 10:30	ワシントンDCおよびバルティモアの(有線および無線)電話回線がトラップドアにより機能不全に陥る。
5月24日 13:30	シカゴの商品取引場で価格が歴史的に変動し、「誰かが取引システムに不正侵入し、価格操作した。」との噂が流れた。
5月24日 午後	ワシントンで緊急に国家安全保障会議が開催されることになったが、電話回線が不通のため、大統領は関係者を召集できない。

注:NCC:National Communications Center
トロイの木馬:あらかじめコンピューターシステムに細工し、自由にそのシステムを操作できるようにするワナ。
トラップドア:パスワード入力やその他のセキュリティ手順を踏まずにプログラムまたはネットワークへのアクセスを許可する方法
出典:"Stsrategic information warfare : a new face of war", Roger C. Molander, Andrew S. Riddile, Peter A. Wilson, Rand Corporation

想像を絶する同時多発テロが起こった現在、上述のシナリオに描かれたサイバー攻撃は現実性を帯びている。次節では、これらのサイバー攻撃の実現可能性を技術的に検証した実験を紹介する。

3.3.2 コンピューターシステムの脆弱性の検証

DODは、1997年6月、DODのネットワークや通信、電力等重要インフラのサイバー攻撃に対する脆弱性を調べるため、「Eligible Receiver」と呼ばれる実験を行った(Testimony by Mr. Richard C. Schaeffer, Jr., October 6, 1999, Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information)。同実験では、国家安全保障関連の機関に勤めるスタッフ30人がハッカーに扮し、以下の課題に取り組んだ。

・通信、電力等重要インフラの管理システムのスイッチ切断
・DODのコンピューターネットワークへの不正侵入

ただし、①通信、電力等重要インフラを攻撃するシミュレーションでは、実際にはスイッチを切らず、証拠となるサインをシステムに残すことが、②DODのネットワークへ不正侵入する実験では、どこまで侵入できるかを明らかにすることが指示された。

ハッカーに与えられた条件は以下のとおりである。

・職業上知り得た知識は一切使わないこと
・利用するコンピューターは、通常の販売店から好きなもの購入すること
・商用のインターネットを利用して攻撃すること
・ハッキングツールは、インターネット上で一般公開されているダウンロードサイトから入手すること

実験に先立ち、3ヶ月の準備期間が設けられたが、ハッカーはこの準備期間に、通信、電力等重要インフラに不正侵入して、管理システムのスイッチを切るサインを残した。また、DODのコンピューターネットワークの不正侵入にも成功している。DODのネットワークへの不正侵入では、テスト回数が4万回、うち侵入に成功したのが36回である。この侵入に対してDODのシステム管理者が検知できたのはたった2回であった。さらに、ハッカーは不正侵入により、DODのすべてのネットワークにアクセスできるシステム管理者としての権限を不正に得ることにも成功している。

この実験から、特別な知識をもたないわずか30名が、通信、電力等の重要インフラを麻痺させ、また世界トップレベルのセキュリティの高さを誇るDODのネットワークを不正に制御できることが分かった。すなわち少人数で米国を国家安全保障上の危機に陥れることができることが判明したのである。この結果は米国政府に大きな衝撃を与え、これを契機に政府内ではサイバーセキュリティ対策が重点課題として取り上げられるようになった。

3.4 米国の重要インフラ防護政策

現在、連邦政府が進めている重要インフラ防護政策のベースとなっているのは、2000年1月にクリントン前大統領が発表した「情報システム防護のための国家計画 Ver. 1.0 ("The National Plan for Information Systems Protection Version 1.0", January, 2000, The White house)」である。

同国家計画は、米国以外の諸外国政府がサイバーセキュリティ政策立案する際に参照されることが多い。

本章では 3.4.1 にて同計画策定までの経緯を振り返った上で、3.4.2 でその概要を紹介する。

3.4.1 情報システム防護のための国家計画 Ver. 1.0 の策定経緯

「Eligible Receiver」実験の結果、DOD のすべてのネットワークは不正侵入の検出装置が備え付けられるとともに、24 時間監視されるようになった。また、DOD 以外の政府機関も、積極的にサイバーセキュリティ対策に取り組むようになった。

一方、政府に比べて民間では重要インフラ防護への取り組みが遅かった。

このため、民間が所有する重要インフラの保護とサービスの安定供給を民間に委ねてきた政府は、民間と協力して重要インフラ防護する方針に切り替え、図表2に示す一連の重要インフラ防護政策を開始した。

図表2 最近の米国における重要インフラ防護政策の変遷

年月	概要
1996 年 7 月	クリントン前大統領が、大統領重要インフラ防護委員会(PCCIP)を設置。
1997 年 10 月	PCCIP レポートの発表
1998 年 5 月	クリントン前大統領が決定指令(PDD63)を発令
2000 年 1 月	情報システム防護のための国家計画 Ver. 1.0 を発表

(1)PCCIP による勧告

1996年7月、クリントン前大統領は大統領令(Exective Order)13010号を発令し、

・PCCIP(大統領重要インフラ防護委員会, President's Commission on Critical Infrastructure Protection)の設置
・上記委員会による重要インフラの定義
・上記重要インフラの防護策の検討

を命じた。

PCCIPは米国の安全保障や国民生活にとって必要不可欠である

・電力供給システム
・ガス/石油生産システム
・金融システム
・通信システム
・輸送システム
・給水システム
・救急サービスシステム
・行政サービスシステム

を重要インフラに指定し、これらを防護するための方策について検討した結果、1997年10月に下記を勧告した。

・民間のサイバーセキュリティに関する意識を高めるため、広範囲にわたるプログラムを開発する
・産官の協力と情報共有を促す
・現行法を見直し、重要インフラ防護の障害となる要因があれば排除する
・重要インフラ防護に適用できる技術を発展させる研究開発プログラムを推進する
・重要インフラ防護に関して、重要決議や勧告を効果的に行うための国家的な取り組みを推進する

これは、政府が重要インフラ防護に関して民間を含めた取り組みについて言及した初めての試みである。

(2)大統領決定指令 PDD63

PCCIPの勧告を受けたクリントン前大統領は、さらにこれにNSCによる検討を加えて、1998年5月にPDD(大統領決定指令, Presidential Decision Directive)63を発令した。PDD63では、以下が命じられている。

・2000年までに政府の情報システムのセキュリティを著しく高め、2003年までに信頼性が高く、安全かつ相互接続した情報システムを構築する。
・早急にサイバー攻撃への警告および対応を行う

国立センターを設置する。
・連邦政府機関がサイバー攻撃や物理的攻撃に対する各自の情報システムの脆弱性を認識し、対策を講じることで、新たな脅威にさらされる機会を減少させる。
・連邦政府が、州政府や民間の手本となるような重要インフラ防御策を講じる。
・官民が協力して重要インフラを防護できるよう民間の自主的な参加を促す。
・個人のプライバシー保護や市場の自由競争を妨げないサイバーセキュリティ対策を実施する。
・サイバーセキュリティ対策全般において、議会へ参加と協力を求める。

さらにPDD63は、図表3に示す体制を構築し、これらの課題に取り組むよう命じている。

図表 3 PDD63 の実施体制

体制	該当者・機関	任務
国家調整官の任命	・初代調整官は、クラーク氏(現連邦政府テロ対策委員会・委員長)。	・大統領によるPDD63の実行を補佐し、国家安全保障、重要インフラ防護および国内外のテロ攻撃に対して責任を持つ。
国家インフラ防護センター(NIPC)設置	・連邦警察に設置され、他にDOD、USSS(米国シークレットサービス)、DOE(エネルギー省)、DOT(運輸省)、インテリジェンスコミュニティ等、コンピューター犯罪やインフラ防衛に関する省庁と民間部門が参加。 ・サイバー攻撃に関する連邦政府の監視センターや民間の情報センター等とネットワークで結ばれている。	・サイバー攻撃の脅威に対する警告、分析、対応策の提示、複数機関による対応の調整、攻撃抑止措置の構築および被害の復旧支援等を行う。
情報共有分析センター(ISAC)設置	・重要インフラ産業ごとにISACを設立する。 ・ISAC第一号は金融業界が設立し、1999年10月からサービスを提供している。	・①サイバー攻撃、コンピューター犯罪等の脅威および被害、②対抗策およびそのベストプラクティス、③システムの脆弱性に関する報告および情報交換。
国家インフラ保証会議(NIAC)設置	・委員長は大統領が直接任命する。 ・委員会の執行取締役は、委員会の執行取締役が兼務する。 ・委員は、大統領が、主要諸機関、国家経済会議(NEC)および国家調整官の推薦に基づき、大手の重要インフラ提供者と地方自治体から任命する。	・定期的に会合を開催し、重要インフラ防衛のため公共と民間セクターの協力関係強化を図る。
重要インフラ保証局(CIAO)設置	・商務省に設置。	・国家調整官による国家の重要インフラ防護政策の立案を支援。 ・重要インフラ産業が策定したセキュリティ対策を国家計画へ組み込む。 ・連邦政府の重要インフラへの依存度を分析。 ・サイバーセキュリティの意識向上プログラムの調整や、関連法案の整備。

出典:PDD63, May 22, 1998, The White House

この PDD63 を具体的な計画に表したのが、次節で紹介する情報システム防護のための国家計画 Ver. 1.0 である。

3.4.2 情報システム防護のための国家計画 Ver. 1.0 の概要

クリントン前大統領は PDD63 に基づき、2000 年 1 月、具体的な計画「情報システム防護のための国家計画 Ver. 1.0 を定めた。

(1)国家計画 Ver. 1.0 の目標

国家計画 Ver. 1.0 は図表4 に示す目標を定めた。

図表4　国家計画 Ver. 1.0 の目標

項目	概要
被害最小化・運用継続化	・重要インフラへのサイバー攻撃による被害を最小化する。 ・サイバー攻撃に遭った重要インフラがダウンせず、機能し続ける。
探知・対応	・タイミングを計ってサイバー攻撃を分離、分析し、さらに攻撃を封じ込め、すばやくシステムを復旧、再構築する。
強固なインフラ建設	・重要インフラへのサイバー攻撃を、国家レベルで回避、検知および対応できるような組織の構築、人材育成、法整備を行う。

(2)国家計画 Ver. 1.0 のプログラム

国家計画 Ver. 1.0 では、(1)の目標を達成するため、図表 5 に示すプログラムが設定されている。

図表5　国家計画 Ver. 1.0 の目標達成へ向けたプログラム

区分	プログラムNo.	概要
被害最小・運用継続	1	重要インフラの構成要素およびそれらの相互依存性を分析し、脆弱性を明確化する。
探知・対応	2	サイバー攻撃と不正侵入を探知する
	3	法的な整合性を確認した上で、重要インフラを防護するため、インテリジェンスコミュニティや捜査当局の執行能力を向上する
	4	サイバー攻撃の警告および対策の情報共有を迅速化する
	5	サイバー攻撃に対する対策、システムの復旧・再構築技術の開発
強固なインフラ建設	6	プログラム1 ～5 を促進する研究開発を支援する
	7	積極的にサイバーセキュリティの専門家を育成、訓練、採用する
	8	サイバーセキュリティに対する市民の認識を高める
	9	プログラム1 ～8 を促進するため、法整備と財政支出を実施する
	10	国家計画Ver. 1.0のすべての項目において、市民のプライバシーおよび財産に関するデータ保護の権利を保護する

出典：The National Plan for Information Systems Protection Version 1.0", January, 2000, The White house

(3)国家計画 Ver. 1.0 を実施する政府機関

図表6に、国家計画 Ver. 1.0を実施する政府機関を示す。図表 6 から、政府は安全保障、研究開発、技術・対策の標準化、人材育成、情報提供・分析等、様々な角度から重要インフラ防護に取り組んでいることが分かる。

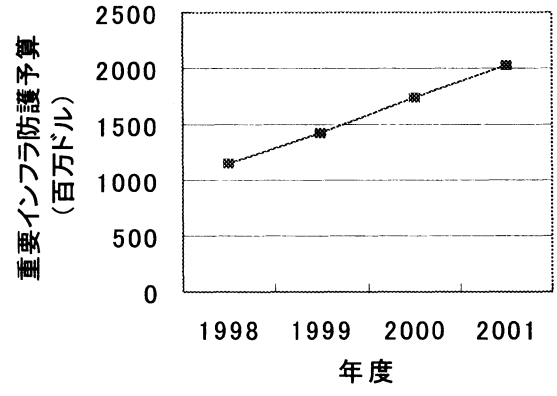
(4)Ver. 2 へ向けて

以上で説明したように、国家計画 Ver. 1.0 では、重要インフラ防護へ向けた連邦政府主導の取り組みが中心になっている。この「Ver. 1.0」というのは、国家計画の構築が初期段階にあり、今後とも進展することを意味している。今後は、民間や地方公共団体が、各自で所有する重要インフラを防護するため、独自に、あるいは政府と共同で果たすべき役割が注目される。現在、ブッシュ政権は国家計画 Ver. 1.0 を踏まえ、議会、州政府、産業界、地域コミュニティあるいは広く一般の意見を取り入れつつ、次期国家計画 Ver. 2.0 を作成中であり、これは今年秋には公開される予定である。

3.5 米国の重要インフラ防護のための政府予算

図表7に米国の重要インフラ防護のための政府予算の推移を示す。

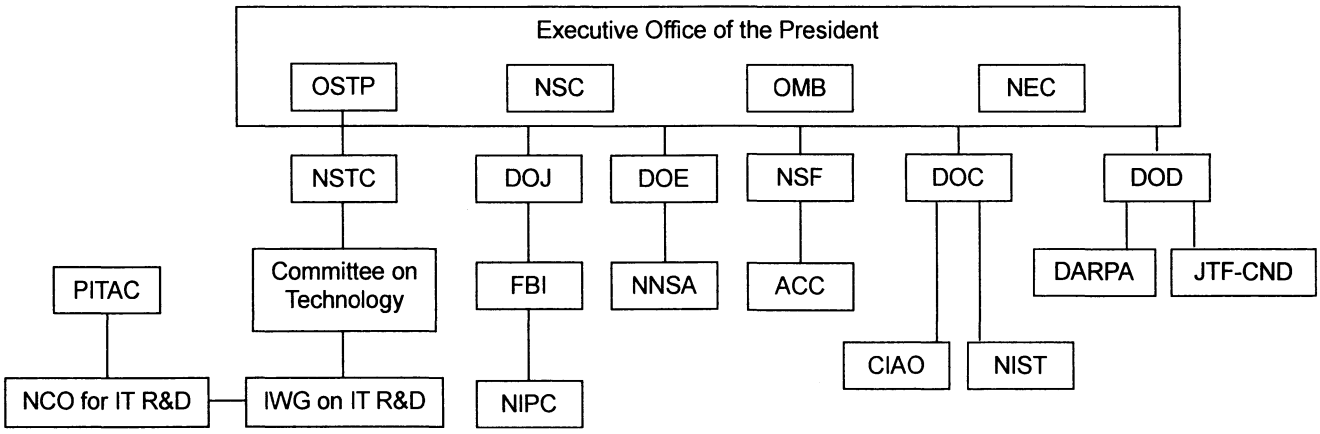
図表7　米政府予算の推移(重要インフラ防護)



出典：Budget of the United States Government、Fiscal Year 2001, Office of Management and Budget, The National Plan for Information Systems Protection Version 1.0, The White House

図表7から米国の重要インフラ防護のための政府予算は順調に増加していることが分かる。

図表6 米国の重要インフラ防護政策の関連組織



機関名

OSTP: Office of Science and Technology Policy

NSTC: National Science and Technology Council

IWG: Interagency Working Group,

PITAC: President's Information Technology Advisory Committee

NCO: National Coordination Office

NSC: National Security Council

OMB: Office of Management and Budget

NEC: National Economic Council

DOJ: Department of Justice,

FBI: Federal Bureau of Investigation

NIPC: National Infrastructure Protection Center

DOE: Department of Energy

NNSA: National Nuclear Security Administration

NSF: National Science Foundation

ACC: Advisory Committee for Cyberinfrastructure,

DOC: Department of Commerce

CIAO: Critical Infrastructure Assurance Office

NIST: National Institute of Standards and Technology

DOD: Department of Defense

DARPA: Defense Advanced Research Projects Agency

JTF-CND: Joint Task Force on Computer Network Defense

3.6 同時多発テロ後のサイバー攻撃対策

10月9日、ブッシュ大統領は現連邦政府テロ対策委員会のクラーク委員長を、新たに大統領サイバーセキュリティ担当補佐官に任命し、①セキュリティが高い情報システムの早急なる構築、②サイバー攻撃の被害を最小化するシステムの構築を命じた("Fact Sheet on New Counter-Terrorism and CyberSpace Positions", October 9, 2001, The White House)。

クラーク補佐官は、任命直後に政府機関のみに使用を限定した専用ネットワーク「ガブネット」の構築計画を発表している("Top Cybercop Wants New Net", October 10, 2001, Associated Press)。

米下院科学委員会では、10月10日、サイバーセキュリティ対策に関する公聴会が開かれ("Committee hears sobering news on nation's cyber security", October 10, 2001, Committee on Science, US House)、サイバー攻撃の脅威を強く懸念する議員や招聘された有識者が、短期、中長期的なレンジで米政府に求められる取り組みについて活発に議論した。

さらに、10月11日付けAP通信は、「米連邦政府は、緊急時に救急作業員と政府職員の通話を優先させる携帯電話システムの構築を計画しており、今後2ヵ月間で500人分、来年末までに5万人分の優先通話回線を確保する予定である。」と報じている("U.S. Plans New Cellular System", October 11, 2001, Associated Press)。

10月16日には、ブッシュ大統領がサイバー攻撃に対する重要インフラ防護命令を発し、①継続的な重要インフラ防護、②非常用通信ネットワークの整備、③大統領重要インフラ防護ボードの設置等を命じた。同ボードは、民間所有の重要インフラ、公的機関の情報システムおよび国家安全保障に関わる情報システムの防護策の立案、調整等を司る米国の最高機関として位置付けられている。

一方、わが国では、10月8日、緊急テロ対策本部の設置が閣議決定されるとともに、同本部がテロに対する緊急対応措置を発表した。この対応措置のうち重点推進事項が10月12日に決定され、「サイバーテロへの対処能力の強化」が一項目に挙がっている。ここでは、具体策として「対処部隊の増強、情報収集、検知・分析・検証機材の増強及び高度化、重要インフラ防護の強化等により、サイバーテロへの対処能力を強化する。」ことが示されている。

また、10月10日、IT戦略本部は情報セキュリティ対策推進会議を開催し、サイバーテロ攻撃に備え、官民の連携強化などを柱とする対処方針をまとめた。

3.7 おわりに

本稿では、サイバー攻撃の脅威が高まる中、早くからサイバーセキュリティ政策を進めてきた米国の取り組みを概観した。

米政府は、世界に先駆けて情報システム防護のための国家計画 Ver. 1.0 を策定し、この実施体制を固めながら、積極的に研究開発、人材育成、法整備、個人のプライバシー保護および予算の支出等に取り組んでいる。特に米政府が、民間や地方公共団体が所有する重要インフラに対して、これらが機能不全に陥ると国家レベルの大混乱が生じるという視点から、積極的に防護政策を進めている点は、わが国にとって大いに参考になる。

ところで、サイバー攻撃の犯人は、自らの足跡を消すために第3者のコンピューターを経由する場合が多く、もし犯人がわが国のコンピューターを経由すると、攻撃された側からは発信地がわが国であるかのように見える危険性がある。すなわち、わが国のサイバーセキュリティの脆弱性が、わが国のみならず他国にも大きなダメージを与え得るのである。

さらに、現段階では、最もサイバーセキュリティ対策が進んでいる米国ですら、重要インフラ防護が十分であるとは言えない。また、ドッグイヤーと言われるように、IT は急激に進歩しており、高レベルのセキュリティ技術を開発しても、すぐ陳腐化する可能性が高い。

このため、わが国は早急にサイバーセキュリティを強化するとともに、絶え間なく対策を更新していくことが重要である。

この点、米国の同時多発テロを契機に、わが国が緊急テロ対策本部やIT戦略本部を中心としてサイバーテロ対策に取り組んでいることは、迅速な対応と言える。

今年秋には米国が国家計画 Ver. 1.0 を更新した国家計画 Ver. 2.0 の発表を予定しており、わが国もこれを参考にしながら、独自の情報システム防護政策を進めていくことが重要である