サイバー戦の現状と展望

―― 「電脳龍」と「電脳鷲」の闘い ――

川　上　高　司

１．米国のサイバー戦

2011年３月、リビアで反政府運動が始まり、英仏を中心とする欧州国がリビア政権勢力に対して空爆を実施する前に、オバマ政権内部では空爆に際しての脅威を除去するためリビアの防空システムへのサイバー攻撃の可否に関して真剣な論議が繰り広げられた。そこでは、リビア政府の軍事上の通信網や早期警戒システムを攻撃してコンピュータネットワークを破壊するかの可否が論議されたのである(1)。しかし議論の末、サイバー攻撃は見送られ、結局巡航ミサイル攻撃を実施した。その理由は次の二点である。第一は、米国が公にサイバー攻撃を実施した場合、その攻撃が前例となり、中国やロシアなどがサイバー戦へ参入する可能性がある。第二は、合衆国の憲法上の問題である。米国では宣戦布告権限は議会にあるが、そもそもサイバー攻撃は戦争という概念にあてはまるのか。そうならば大統領は議会の許可なくサイバー攻撃できるのか否かという憲法上の問題である。

さらに2011年５月２日のオサマ・ビン・ラディン襲撃に先立ち、やはりサイバー攻撃の是非を巡りオバマ政権内で議論がなされた。米海軍の特殊部隊を乗せた輸送機がパキスタン領空内を移動飛行する際にパキスタンのレーダーシステムに対するサイバー攻撃を行なるか否かの議論が行われ、実施は見送られた。その代替としてステルス性ヘリコプターが使われた。このステルス性ヘリコプターは現場で墜落したためその存在が明らかになり注目を浴びた。

世界中でインターネットやコンピュータなどサイバー空間へ依存する社会システムが構築されるにつれ新たな戦争形態が生まれ､そこでの戦域は軍事以外のところへも拡散する。2010年には、グローバルなハッカー集団である「Anonymous（匿名集団)」が、ネット上で好戦的な攻撃を繰り返した。ウイキリークスを主宰するジュリアン・アサンジの逮捕に対する報復としてAnonymous は12月８日にはマスター・カード社のシステムをダウンさせ、VISA社やペイパル社、スエーデンの検察サイトをもシステムダウンさせるなど、サイバー戦を予感させるような事件を引き起こした。

また同年、イランの核開発施設ではコンピュータがスタクスネットワーム （Stuxnet computer worm）に侵されてシステムダウンしその開発プロセスが遅れるという事態も起こったが、このウイルスはイスラエルとアメリカの共同開発したものだと言われている(2)。ウイルスを誰が作成したにせよ、サイバー上では他国の核開発をも妨害できる事実が明らかになったのである。

以上の例は氷山の一角にすぎず、サイバー攻撃は頻繁に行われ、携帯電話のシステムダウンから核開発まであらゆるところへの攻撃が可能である。しかも被害の程度からその規模脅威のレベルもさまざまで、戦場がサイバー上であるため人々の認識が薄い。このこと

からオバマ政権は米国内で2011年10月を「サイバーセキュリティPR月間」と定め、サイバーセキュリティの周知と理解を深める取り組みをした(3)。

2．サイバー戦の現実
―サイバー・ドラゴン(電子龍・中国)の暗躍

2009年６月23日、オバマ政権は国防総省の組織内にサイバー司令部（United States Cyber Command）を新設して国防の最前線に参戦させた。2010年のホワイトハウスの国家安全戦略では「サイバーセキュリティは国家安全保障の中で最も脅威の高いものの一つである」とサイバーセキュリティの重要性を述べている。そして、2011年の国防予算審議では厳しい予算削減にもかかわらずサイバーセキュリティ関連の予算は削減の対象にはならなかった(4)。アメリカがサイバー防衛だけでなく攻撃能力の向上にも力をいれていく戦略が読み取れる。そこで、サイバーセキュリティの現状と展望をアメリカの国防戦略と論じる。

また、本論文では、サイバー空間とは「コンピュータやデータ通信によって相互に人間同士がつながるが、そこには物理的な存在はない状態」と定義する(5)。現在世界中でネット上にあるコンピュータはどこかで相互につながっている。その瞬間にそこにはサイバー空間が形成されていると見ることができる。そのような物理的に存在しない空間では電子情報が飛び交い、その電子情報をめぐっての攻防が繰り広げられる。本論文ではサイバー戦（cyberwarfare）とは「コンピュータを用いて他のコンピュータやネットワークを電子的に攻撃する、あるいは防衛すること」と定義する(6)。この場合、攻撃や防衛主体は国家、個人、集団、組織などあらゆる形態が考えられる。

2011年８月３日、米国のコンピュータ・セキュリティ会社のマカフィーは、過去5年間にわたって起こった高度なサイバー攻撃に関する報告書を発表した。その報告書によれば同社は世界中で72個のサイバー攻撃を確認し、そのうち米国は49回の攻撃を受けた。内訳は14回が政府や州政府の関係、11が国防コントラクター、その他には司法関係の省庁も攻撃対象となった(7)。米国の他にはアジア地域では日本、台湾や韓国、ベトナム、インド、インドネシア、香港、シンガポールが被害を受け、その他の地域ではカナダ、スイス、英国、デンマーク、ドイツが被害を受けたと報告された。さらに国際オリンピック協会、国連、ASEANなどもサイバー攻撃を受けたとされる(8)。日本では2011年にソニーがサイバー攻撃を受けて顧客情報が流出した事件が起こった。これら一連のサイバー攻撃をマカフィー社のドミトリー・アルペロビッチ副社長は「隠れネズミ作戦（Operation Shady

RAT)」と名付けて、2010年に起こった「オーロラ作戦（Operation　Aurora)」に匹敵する脅威を与えかねない危険なサイバー攻撃と位置づけた。オーロラ作戦とはグーグル社をはじめとする企業が攻撃を受けてダメージを被った事件である(9)。

これらの大規模で高度なサイバー攻撃の実行者についてはCSISの専門家ジェイムズ・ルイスは「すべての兆候（サイン）が中国を示している」と述べている(10)。当然ながらサイバー攻撃の実行者を特定することは困難であり中国から攻撃が行われているという判断は推測にすぎない。サイバー戦の困難さは攻撃主体を特定することの困難さに起因する。

2011年初頭、RSAという米国のEMC社のセキュリティ部門がサイバー攻撃を受けた。RSAはCIAやNSA（国家情報局）や国防総省などの政府機関(11)やロッキード社、カンザス州、イギリス地方自治体などにサイバーセキュリティを提供している(12)。そのセキュリティ部門から顧客のID情報がサイバー攻撃により盗まれるという前代未聞の事態が起こった。そしてそのIDを使って顧客のコンピュータシステムが侵入を受け企業情報が盗まれた。続いて５月には国防企業のロッキード社がセキュリティを破られてオバマ大統領が事態を憂慮するに至った。この直後には情報や監視技術を提供する国防コントラクターのL-3社（L-3　Communications）が攻撃を受けた。その翌日にはノースロップ社が攻撃を受けたためシステムをシャットダウンして大混乱に陥った。

このように中国からのハッキングやスパイ行為は10年ほど前から活発になり、その技術はセキュリティを提供する企業ですらサイバー攻撃の対象となるほどにより洗練され高度化しつつあり、大きな脅威となっている。その姿はまさに「電脳龍」（cyber-dragon）である。

これまではサイバー攻撃の防戦が主体だったアメリカもこのように繰り返し深刻な攻撃を受けるに至ってようやく動きだした。軍はサイバー攻撃に消極的だったがついにサイバー戦略を立てる方向で動きだした。サイバー司令部を有する戦略司令部（U.S. Strategic Command）のロバート・ケラー司令官は従来の陸・海・空でのドクトリンではない新たなドクトリンの必要性を強調している(13)。サイバー空間は現実の戦場とは異なり国境もなくグローバルに広がっている。またそのテクノロジーは日々刻々と進化しており、ドクトリンもそれにあわせて柔軟に進化していかなければならない。伝統的な手法は通用しないため、全く新しい手法を開発するところからスタートしなければならないのである。ついにCyber-Dragon（電脳龍・中国)とCyber -Eagle（電脳鷲・米国）の闘いが本格的に開始されたのである。

３．米政府のサイバー戦への取り組み
―サイバー・イーグル（電子鷲・米国）の始動

2008年１月、ブッシュ政権は国土安全保障大統領令23と国家安全保障大統領令54により、米国がサイバー上の脅威に対する防衛強化を行う「包括的サイバーセキュリティ構想（Comprehensive National　Cyber security Initiative(CNCI)）」を発令した。詳細は機密であったが部分的に伝えられたことは、CNCIは政策や戦略、ガイドラインを作りより高度な技術や能力の向上を目指すことがその任務であり12項目の目標(14)が定められたとされている。これを踏まえて国土安全保障省（DHS）において、NSA、FBIと連携して国家全体のサイバーセキュリティーを総括するNational Cyber Security Center(NCSC)が設置され、ロッド・バックマン(15)が任命された(16)。

オバマは大統領選挙期間中からサイバーセキュリティーの強化を訴え、国家サイバーアドバイザー（National Cyber Adviser）の設置を約束していた。

また、オバマ大統領はCSIS（米国際戦略研究所）の「サイバーセキュリティ委員会」の提言（８項目）に沿い2009年２月９日、サイバーセキュリティー政策のレビューを開始し、４月17日に提出された(17)。そして、そのレビューを踏まえて５月29日に「60日間のサイバーセキュリティ政策の見直し」を発表した。そこでは、サイバーセキュリティーを経済繁栄、安全保障の基盤であるとし、サイバー攻撃が軍事のみでなく経済的にも脅威であると明確に位置づけた。その発表の際には、オバマ政権は横割りのサイバーセキュリティ政策や戦略調整をとして新たに「サイバー・コーディネーター（Cyber Coordinator)」(18)を創設した(19)。そこでは、サイバーセキュリティー政策のとりまとめをDHSからホワイトハウスに移管した。サイバー・コーディネーターには国家安全保障担当補佐官、国家経済会議議長への報告義務が課せられ、大統領との直接の会見ができる。サイバー・コーディネーターに国家経済会議への報告が義務づけられたことは、サイバー戦が軍事上だけでなく経済上も闘われることを意味する。

そして、2009年12月に初代のサイバー・コーディネーターにハワード・シュミットを任命した。シュミットは、2001年から2003年の間はブッシュ大統領の特別アドバイザーを務めていた。シュミットは空軍に属していた後、1990年代はFBIで麻薬情報センターに属していた。その後マイクロソフト社、eBayを経てブッシュ政権入りを果たした。ブッシュ政権を去った後は情報関連の非営利団体を主宰していた(20)。サイバーセキュリティは国防総省を含めてあらゆる省庁にまたがっているためサイバー・コーディネーターがどこまでそれらを束ねて調整できるかが鍵となる。その意味ではシュミットの責任は重く、国土安全保障省は非軍事部門の省庁を率いる役目を担う(21)。

2012年１月５日にオバマ大統領が発表した新国防戦略では、米軍の増強すべき分野として対テロ、非対称戦、抑止および紛争の撃破、敵国のA2AD（接近拒否・領海拒否）に対するパワープロジェクション、対WMD（大量破壊兵器)、安全で確実な核抑止の維持、本土防衛と文民活動家支援、プレゼンス維持、安定と対COIN（対反乱安定作戦)、人権と災害救援と並んで、宇宙及びサイバー空間での優位を挙げた。さらに同戦略では、「サイバー戦、特殊作戦、情報収集、偵察能力の強化が米軍の競争力を維持する」と述べている。米軍は素早く正確で効果的な作戦の遂行には正確な情報と通信ネットワークが不可欠である。つまりサイバー空間へのアクセスが保障されなければならないと、サイバー空間の軍事的な重要性を強調している。そしてサイバー空間の安全性を高めるために国防総省は国内外で協力体制を敷きながらサイバーセキュリティの向上に努めると方向性を示した(22)。アメリカ合衆国すなわちサイバー・イーグル（cyber-eagle)「電脳鷲」が、 サイバー空間に躍り出てきたのである。

４．国防総省の取り組み―サイバー司令部の創設

2009年６月23日、ロバート・ゲイツ国防長官は、戦略司令部（U.S. Strategic Command）司令官に対してサイバー司令部（U.S. Cyber Command）の創設を指示しサイバー司令部（USCYBERCOM）が創設された。実際の稼働は2010年５月と定められ本部はメーデ基地に置き、およそ1000人の文民と軍人が配置された。初年度の予算は１億2000万ドル、2011年は１億5000万ドルである(23)。

サイバー司令部が創設される以前は、サイバー防衛に関しては統合タスクフォース・グローバル・ネットワーク作戦部（Joint Task Force Global Network Operations）が担い、サイバー攻撃に関しては統合ネット戦争機能司令部（Joint Functional Component Command Net Warfare）が担っていた(24)。しかし防衛と攻撃はコインの表と裏（pros and cons）の関係にあり別個の組織で運営することはきわめて非効率であるとの認識に立ち、統合してサイバー司令部を立ち上げ、今後激化すると予測されるサイバー空間での攻防に備える。

国防費の2012会計年度予算法では、サイバーセキュリティの能力の向上、国土安全保障省との協力体制の整備、そしてサイバー攻撃に関する条項が盛り込まれた。サイバー攻撃に関しては先述したように宣戦布告権限という憲法上の問題点がリビア空爆の際に浮上し結論がでなかったが、2012年の予算法では政策の原則と法律の枠組みの範囲内で大統領令、あるいは大統領の戦争権限決議によってサイバー攻撃を国防総省は実施することが

できると定めた(25)。

これによって、アメリカは大統領の命令でサイバー攻撃を実施することが可能となった。これは、時間の優位性において大きな前進となる。今後、軍時作戦上でリビア空爆やオサマ・ビン・ラディン襲撃のような作戦が実施される際には軍は躊躇なくサイバー攻撃を実施でき、より効率よく敵を叩くことが可能になる。最も直近で実施の可能性が考えられるのは、未だ民主化運動が激しく続いているシリアである。シリアへの介入にはアメリカは慎重な姿勢を崩さないが、リビアのように空爆の実施を仮定するならば事前のサイバー攻撃によって国防システムに打撃を与える可能性は高い。それによって最小限の被害と最小限の投資によって最短期間で戦局を決することができる。

サイバー司令部の初代司令官はケイス・アレキサンダー陸軍将軍が就任し、国家安全保障局（National Security Agency）局長、中央安全保障部（Central Security Service）部長も兼務する。ケイス・アレキサンダー陸軍将軍は長年陸軍の情報部門に属してきた人物である。

国家安全保障局は1952年にハリー・トルーマン大統領によって設立された。国家安全保障局は暗号と情報の保全を任務としてきた(26)。それはネットワーク社会になるにつれますます重要性が増し、特に情報保全の問題はサイバー空間という新たなドメインでも重要である。中央安全保障部は1972年の大統領令によって創設された。中央安全保障部長は国家安全保障局長と兼務することになっており、任務も共同作業であることがほとんどである。中央安全保障部には軍事上の要素が加わる点がNSAとは異なる。中央安全保障部の任務は最前線への部隊への支援などであり4軍とのつながりが強い(27)。

ただし、実際の任務は別々に遂行される。サイバー司令部は戦略司令部の下に作られ、構成するのは、陸軍サイバー司令部（Army Forces Cyber Command)、第24空軍(24th USAF)、艦隊サイバー司令部（Fleet Cyber Command)、海兵隊サイバー司令部（Marine Force Cyber Command）と、国土安全保障省の沿岸警備隊サイバー司令部（Coast Guard Cyber Command）である。

2011年７月国防総省は「サイバースペース運用の国防戦略（Department of Defense Strategy for Operating in Cyberspace)」を発表した。2000年には３億6000万人だったインターネットの利用者が2010年には20億人に増加した。日々ネット利用者は増え続けており、サイバー空間にはあらゆるインフラや情報が交錯している。しかしその一方でサイバー空間は脆弱で､特に米国のサイバー空間は国内外からのサイバー攻撃にさらされている。特に重要なインフラへのサイバー攻撃は最も高い脅威の一つであると、この国防戦略では位置づけている。つまりサイバー空間のセキュリティを強化することが国家の防衛と同様の意味をもつが、目に見えない空間での目に見えないセキュリティはこれまでの概

念では対応できない。新たなセキュリティ概念が必要なのである。

国防総省は５つの方針を打ち出した。第１に、サイバー空間を陸・海・空・宇宙に続く「第５の領域」とみなす。すでに「サイバー司令部」を立ち上げて稼働しているが、今後サイバー部隊は陸軍、海軍、空軍、海兵隊に続く「第５の軍種」と位置づけられるようになるかもしれない。第２に、ネットワークシステムの防衛のために新たな防衛作戦コンセプトの構築をする。その前提としてこれまでのように作戦コンセプトを固定するのではなく、コンセプトそのものを常に進化させていかなければならない。そして常にネットワークを進化させていかなければならない。第３に、他の省庁や企業と協力して国家全体のサイバーセキュリティを構築する。特に国土安全保障省との協力・連携が求められるだけでなく、国防企業とも協力体制を盤石にしなくてはならない。第４に、同盟国との関係を構築して「集団的サイバーセキュリティ」を強化する。サイバー空間の本質はグローバルであるため多国間での同盟関係や協力体制はセキュリティ向上のためには不可欠である。しかし、現実世界で認められている集団的自衛権をそのままサイバー空間に適用できるかどうかについては国際社会での議論が必要である。第５に、優れた人材や技術革新によって国家としての優越性を高める、と５つの方針を打ち出した(28)。

５．対テロ対策としてのサイバーセキュリティ

サイバー戦は経済的側面の他には、対テロ対策という軍事的な側面も持つ。米国が注目しているのが、アルカイダやタリバンなどイスラム過激派グループとインターネットの関係である。近年アルカイダはその活動においてインターネットを駆使しておりそれが見過ごせない脅威となりつつあると国防総省は認識している。

アルカイダはインターネットをその活動において十二分に活用している。ウエブサイトを開設してプロパガンダ、リクルート、イメージ戦略やテロの手法、テロの標的の情報から爆弾の作り方、サイバー攻撃の方法などあらゆる情報を提供している。特に英語のオンライン誌「Inspire」を通じて英語圏でのプロパガンダにも積極的になっているといわれている(29)。「Inspire」とアルカイダの関係を疑問視する意見もあるが(30)、同誌が「台所の母親を吹き飛ばす方法」という類の記事を掲載していることから、穏健なオンライン誌でないことは確かである。このオンライン誌を編集していたのはパキスタン系米国のサリム・カーンで2011年９月29日のイエメンでのCIAによる空爆によって米国に殺害されている。

米国が密かに注目してここ２年ほどの間追跡していたのが、この「Inspire」誌にも執

筆し、英語圏でのプロパガンダに絶大な影響力を持っていたとされるアンワル・アル・アウラキである。アウラキはイエメン人を両親にもち米国で生まれ、大学教育まで受けた。在学中には説教師として2001年9.11テロの実行犯のうちの２名と会っている。2004年にはイエメンに戻り、その英語能力を駆使して反米思想を伝搬することに尽力していた。彼のネット上の講義や説教は多くのイスラム教徒に影響を与えたとされる。2009年にテキサスのフッド基地内で13人の犠牲をだした銃乱射事件の容疑者もアウラキの説教を受けていた。2010年５月にタイムズスクエアで爆破事件を実行しようとしていた容疑者もまたアウラキの影響を受けていたとされている(31)。

ここ数年の特徴として、アメリカ国籍のイスラム教徒がアメリカ国内でテロを起こそうとする傾向が顕著だが、そこにはこのようにネットを利用した洗脳が行われており、遠く離れた地域からでも簡単にテロリストを養成できるようになっている現実がある。外国でテロリストをどれだけ殺害しても国内でテロリストが生まれているような状況が今後さらにエスカレーとしていくと、アメリカはより高い脅威にさらされることになる。アメリカがサイバーセキュリティに力を入れる理由の一つはここにある。テロとの戦争は現実の戦争に加えてサイバー空間にも戦場が拡大しているのである。

アラウキは、米軍の追跡を受けて2011年９月29日にCIAの空爆によって殺害された。だが、この殺害は若いイスラム教徒の反米感情をさらに煽るだけでかえって逆効果だという指摘もある(32)。オサマ・ビン・ラディン殺害はその名声を高めイスラム教徒の間で反米感情を盛り上がらせる結果となっている。それと同じようにアラウキが米国に殺害されたことによって名声が高まりその思想が広まる危険がある。それはネッを通じて瞬時に爆発的に拡散するとの指摘もある。

さらにサイバー空間はテロリストの資金調達でも活躍している。テログループは、サイバー空間の地下組織やハッカー集団ともつながって資金調達、武器密輸、麻薬密輸など、現実世界と変わらない違法行為がより簡単に行われておりその実態もつかめない。そのためテロ組織はより簡単に資金調達や資金洗浄をすることができるようになっている。この資金の流れを絶つこともまた、テロを撲滅するためには必要不可欠な任務である。そのためにはサイバー空間で監視体制を強化する必要がある。

サイバー空間で得られた情報からテロリストを追跡して拘束・殺害する作戦が今後は対テロ対策の主流となる可能性がある。イラクやアフガニスタンから地上部隊を撤退させ、無人偵察機や監視衛星、ネットの監視などサイバー空間での監視を強化し標的を定めて少数精鋭の特殊部隊によるピンポイント攻撃あるいはCIAによる無人爆撃機による暗殺という、サイバー戦と現実での攻撃とを組み合わせた作戦を米軍は多用していく可能性が高い。厳しい予算削減は米軍の戦略にも影響を与えている。大規模な地上部隊を送らない一方で

サイバー空間での作戦とのコラボレーションで効率よく闘う方向へと米軍は転換しようとしている。オサマ・ビン・ラディンの襲撃の際仮に事前にパキスタン側にサイバー攻撃を行っていたら、まさにそれこそが米軍の目指している戦闘となったに違いない。

６．今後の課題

サイバー空間は「第５の戦域」と国防総省が位置づけるように、そのドメインは益々重要になってきている。しかし国内外での議論が十分でなく、国際社会でのルールやコンセンサスも確立していない。サイバー戦のその被害程度も多岐にわたり国家だけでなく市民生活に深刻な被害をもたらすことも可能があるだけに、国際社会での議論とコンセンサスの確立が急がれる。本稿では以下５点を提言したい。

第１に、従来の概念にとらわれない戦略やドクトリンを確立する必要がある。サイバー戦攻撃の主体や目的は多様で多岐にわたる。主体は国家、個人、集団あるいは組織とあらゆる形態が考えられる。サイバー攻撃のその目的も経済的、軍事的、政治的などと多様であるため、攻撃対象も多岐にわたる。第２に、サイバー戦と法の整合性を確立しなければならない。第３に、攻撃と防衛の定義である。たとえば国家システムへの攻撃は宣戦布告とみなすのか、その場合自衛権や先制攻撃は認められるのか。第４に、攻撃対象をどこまで許容するか。現実の戦争の場合は戦闘の対象は軍用に限られ民間人や民間施設は対象にしてはならない。果たしてサイバー戦ではこのような区別が可能なのか。それはサイバー戦の場合は被害の広がりが無限ともいえ、民間への被害は避けられない事が多いからである。第５に、サイバー空間への規制が行なわれたり、個人への監視が行われたりするようになると個人の自由やプライバシーと抵触する。個人情報の保護とのバランスをとることが必要となろう。

世界はグローバル化して情報面でも互いに絡み合っている。サイバー攻撃は、サイバー空間がいかに脆弱であり、ネットがグローバルなゆえに被害も多国間にわたる危険性を大きくはらんでいる。個人の情報や国家レベルの情報が地球の裏側へも簡単に流出する時代に突入したのである。自国のファイアーウオールを強化するだけでは守り切ることは不可能になってきている。日本も米国とともにセキュリティを高めていく必要がある。国防総省の戦略でも「同盟国との協力」が強く打ち出されている。

サイバー空間を通じたネット社会の形成は大きく社会を変える力を持っていることが2011年のアラブの春や民主化運動を通じて明らかになった。インターネットがなければおそらく民主化運動はもっと時間がかかったかもしれないし、成功しなかったかもしれな

い。一方で企業や政府機関は日々サイバー戦の脅威にさらされており、情報の保全が困難な時代になっている。

その中でもサイバー空間で存在感を持ち始めた中国＝サイバードラゴン（Cyber-dragon）と、サイバー空間でのプレゼンスの高まりを狙う米国＝サイバーイーグル（Cyber-eagle）が熾烈な競争を繰り広げるであろう。まさに2012年はサイバー戦時代の幕開けである。

注

（1）“U.S. Debated Cyber warfare in Attack Plan on Libya”, Erick Schmitt and Thom Shanker, The NewYork Times, October 17,2011 (http://www.nytimes.com)
（2）“U.S. Debated Cyber warfare in Attack Plan on Libya”, Erick Schmitt and Thom Shanker, The NewYork Times, October 17,2011 (http://www.nytimes.com)
（3）“WH Proclaims ‘cyber-security awareness month’”, October 3,2011 (http://www.dodbuzz.com)
（4）“Senate Armed Services Committee Completes Conference of National Defense authorization Act for Fiscal Year 2012”, Dec 12,2011 (http://armedsercies.senate.gov)
（5）“Cyberwarfare”, Steven Hildreth, June19,2001, CRS Report for Congress
（6）“CYBER WARFARE- An Analysis of the Means and Motivations of Selected Nation States”, Charles Billo and Welton Chang, Institute for Security Technology Studies at the Dartmouth College, November 2004 (http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf)
（7）“Security Firm Sees Global Cyberspying” David Barboza and Kevin Drew, New York Times, Aug.3,2011(http://www.nytimes.com)
（8）“Exclusive: Operation Shady RAT Unprecedented Cyber-espionage Campaign and Intellectual Property Bonanza”, Michael Joseph Gross, Vanity Fair, August 2,2011 (http://www, vanityfair.com/cuture/features/2011/09/operation-shady-rat-201109)
（9）“Exclusive: Operation Shady RAT Unprecedented Cyber-espionage Campaign and Intellectual Property Bonanza”, Michael Joseph Gross, Vanity Fair, August 2,2011 (http://www, vanityfair.com/cuture/features/2011/09/operation-shady-rat-201109)
(10) “Exclusive: Operation Shady RAT Unprecedented Cyber-espionage Campaign and Intellectual Property Bonanza”, Michael Joseph Gross, Vanity Fair, August 2, 2011 (http://www,vanityfair.com/cuture/features/2011/09/operation-shady-rat-201109)
(11) “Enter the Cyber-dragon”, Michael Joseph Gross, Vanity Fair, September, 2011 (http://www.vanityfair.com/culture/fearues/2011/09/chinese-hacking-201109)
(12) http://www.rsa.com
(13) “U.S. Weighs Its Strategy on Warfare in Cyberspace” Thom Shanker, New York Times, October 18,2011 (http://www.nytimes.com)
(14) Trusted Internet Computing, Intrusion detection, Intrusion prevention, R&D, Situational awareness, Cyber counter intelligence, Classified network security, Cyber education and training, Implementation of information security technologies, Deterrence strategies, Global supply chain security, Public/private collaboration.
(15) シリコンバレーの起業家
(16) DHSは、CNCIに基づき、US-CERTの人員拡充、EOMSTEINプログラムの拡充、外部関連の統合、National Cyber Security Center Centerの創設、National Cyber Investigative Joint Task Force(NCIJIF)の他省庁への拡充、NIPPに基づく官民での情報共有、Cyber Storm IIの実

施、サイバー教育の拡充、連邦のIT予算の拡充、を行った。
(17) このレビューにはODNIのCyber Coordinaion ExecuiveをつとめていたMelissa Hathawayがホワイトハウスの Senior Director for Cyberspace代行として取り組んだ。
(18) 通称として「サイバー長官（Cyber Czar)」と呼ばれることもある。
(19) “Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress”, Catherine A. Theohary and John Rollins, Jan.12,2010, CRS Report for Congress, R40836(http://www.crs.gov)
(20) “Obama to name Howard Schmidt as cybersecurity coordinator”, Decmber 22,2009, Washington Post (http://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html)
(21) “Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress”, Catherine A. Theohary and John Rollins, Jan.12,2010, CRS Report for Congress, R40836 (http://www.crs.gov)
(22) “Sustaining U.S. Global Leadership: Priorities for 21st Century Defense”, January , 2012
(23) “Alexander Details U.S. Cyber Command Gains”, Sep.24,2010 (http:www.defense.gov/news/newsarticle.aspx?id=61014)
(24) “Alexander Details U.S. Cyber Command Gains”, September.24,2010 (http:www.defense.gov/news/newsarticle.aspx?id=61014)
(25) “Senate Armed Services Committee Completes Conference of National Defense authorization Act for Fiscal Year 2012”, Dec 12,2011 (http://armedsercies.senate.gov)
(26) http://www.nsa.gov/about/faqs/about_nsa.shtml#about3
(27) http://www.nsa.gov/about/faqs/about_nsa.shtml#about3
(28) “Department of Defense Strategy for Operating in Cyberspace”, Department of Defense, July 2011
(29) “Two-Year Manhunt Led To Killing of Awlaki in Yemen”, Mark Mazzetti, Eric Schmitt and Robert F. Worth, New York Times September 30,2011, (http://www.nytimes.com)
(30) “Terrorist Use of the Internet: Information Operations in Cyberspace”, Catherine A. Theohary and John Rollins ,March 8,2011, CRS report for Congress, R41674
(31) “Two-Year Manhunt Led To Killing of Awlaki in Yemen”, Mark Mazzetti, Eric Schmitt and Robert F. Worth, New York Times September 30,2011, (http://www.nytimes.com)
(32) “Two-Year Manhunt Led To Killing of Awlaki in Yemen”, Mark Mazzetti, Eric Schmitt and Robert F. Worth, New York Times September 30,2011, (http://www.nytimes.com)