「アジア太平洋の新秩序」研究会　第９回研究会　議事要旨

１．開催日時：平成２７年７月１６日（木）１８：００－２０：００

２．開催場所:東京財団 会議室Ａ(東京都港区赤坂１－２－２日本財団ビル３階)

３．出席者（敬称略）　※共同主査

委員

・秋山昌廣※　東京財団理事長
・川口順子※　明治大学研究知財戦略機構特任教授/東京財団名誉研究員
・伊藤　剛　　明治大学政治経済学部教授
・小島　明　　日本経済研究センター参与
・林　良造　　明治大学国際総合研究所長
・平沼　光　　東京財団研究員
・森　　聡　　法政大学法学部教授
・門間大吉　　財務省国際局長
・渡部恒雄　　東京財団政策研究ディレクター(外交・安全保障担当)

事務局

・鎌江一平　　事務局長補／明治大学国際総合研究所共同研究員
・花田美香子　事務／東京財団政策研究アシスタント
・和田大樹　　事務／東京財団リサーチアシスタント

４．配布資料

- 議事次第
- 研究会出席者リスト
- 2015 年度「アジア太平洋の新秩序」研究会概要
- 土屋大洋氏講演資料「情報と安全保障」
- 土屋大洋氏略歴

５．議事（要旨）

（１） 講師講演

講師：土屋大洋（慶應義塾大学大学院政策・メディア研究科教授 兼
総合政策学部教授）

テーマ：米中の相互依存関係とサイバーセキュリティ

<u>サイバーセキュリティのアトリビューション（帰属・属性）問題</u>

- 2012 年 10 月 25 日、NY Times 紙が温家宝の不正蓄財を報道。これを契機に、中国のサイバー攻撃が米 IT・メディア企業、米政府に対して急増した
- 2013 年 2 月、米コンピューター・セキュリティ企業 Mandiant 社が報告書で、上海のビルを拠点に人民解放軍「第 61398 部隊」が世界中をサイバー攻撃していると指摘。これを NY Times 紙が報じた。
- 2013 年 6 月、米中首脳会談が米カリフォルニアにて開催されるも、スノーデン問題の影響もあり、サイバー問題に関して合意には至らず。
- 2014 年 5 月、米司法省が会見で米・加企業へのサイバー攻撃によって企業秘密を盗んでいるとして「第 61398 部隊」所属の人民解放軍当局者 5 名を実名・顔写真付きで公開。米連邦捜査局（FBI）は 5 名を訴追した。これに中国は強く反発し、米中の政府間でのサイバー対話を中止。
- 2014 年 7 月、米コンピューター・セキュリティ企業 CrowdStrike 社が報告書を発表。その中で、中国人民解放軍総参謀部第三部の傘下にあり上海に拠点を置く「第 61486 部隊」のハッカーを特定できたとして関連する個人情報を公開。
- 2014 年 12 月、映画「インタビュー」（金正恩等北朝鮮を風刺した映画）の公開を差し止めるべくソニーピクチャーズ社に対してサイバー攻撃が行われた。通常、攻撃の発信源を特定するのに数か月を要するアトリビューション問題においてわずか 1、2 週間で FBI が北朝鮮であると判定。
- 2015 年 2 月、中国は中国の金融機関が国内で金融取引に使用する暗号ソフトを国産にすると発表。外国製のソフトウェアを使用する場合にはソースコードを開示し「バックドア」を作成し、中国政府によるアクセス可能を義務付けるとした。これは、米国企業の取引を事実上困難にするとして貿易問題に発展しつつある。同月、オバマ大統領はスタンフォード大学でのサイバーセキュリティサミットに参加。この問題に対する米国政府の憤りを示した。
- 2015 年 4 月、上記を受けてオバマ大統領は大統領令を発令し、サイバーセキュリティの分野での国家非常事態を宣言している。

三つのタイプのサイバー攻撃

① 分散型サービス拒否攻撃（DDoS: Distributed Denial of Services）

世界中の第三者にウイルスをばらまき、そのウイルスを特定のターゲットに向けて機動させ、アクセスを殺到させるというもの。物理的破壊攻撃による被害が生じるわけではないが、ネットワーク上のアクセス障害が起きるために際立って迷惑な行為となる。したがって、メディアの慣用ではしばしば「cyber attack（攻撃）」とされるが、国際法上厳密には attack に分類されず「cyber operation」に分類される。WMD（=Weapons of Mass Disturbance）と揶揄されることもある。

2007 年、エストニアで首都タリンの広場にあるソ連由来のブロンズ像を移転するに当たってロシアでの報道直後から DDoS がエストニアに対して一斉に起きた。

② 高度で執拗な脅威（APT: Advanced Persistent Threat）

「標的型電子メール攻撃」とも言われることが多く、電子メール等を通じて情報を盗み出すことが多いが、必ずしも電子メールには限られない。APT によるウイルス侵入後、中間値として 229 日気づかないという統計データがある。最長記録として被害にあったことに 2,287 日気づかなかったケースもある。APT により、昨年までの段階で 3 億種類のウイルス、マルウェアが存在すると推計されている。ウイルス対策ソフトのウィンドウ・ピリオド（1 週間程度）やカスタマイズされたウイルスなどを考えると対抗策を立てるのが難しい。

一例として、Backshot Yankee 作戦が挙げられる。これは、米軍の駐車場に落し物を装いばらまかれた USB を拾った隊員たちが米軍 PC にその USB を接続し、ウイルスの侵入を許し、米軍のネットワークが乗っ取られた事件。

日本では、2011 年 3 月 11 日の東日本大震災の 20 日後に各省庁へ向けて「昨日の放射線レベル」と題した電子メールが送られてきた。添付ファイルを開くと「カスタマイズ（＝ウイルス対策ソフトウェアが有効でない）」されたウイルスに感染し、リモートコントロールによる広範囲な政府情報の搾取が広範で行われた。同年 9 月に三菱重工において、セキュリティ対策を施していない外郭団体を通じてネットワークが乗っ取られる形で被害を受けた。

2014 年 9 月、JP モルガンが 1 兆円規模のサイバーセキュリティ対策を施そうとする中、同攻撃で狙われた。

③ 通常兵器・サイバー組み合わせ型攻撃（CCC: Cyber-Conventional Combination）

2008 年、イスラエルがシリア国内に所在する北朝鮮系の核施設を衛星写真で捉え、シリアによる核開発疑惑が高まる。イスラエルはブッシュ大統領に

電話をし、空爆を要請。米国は拒否したが、イスラエルが空爆を実行したと見られている。その際、シリアの防空網が破られたのはイスラエルが事前にレーダー網をサイバー攻撃で操作していたためと言われる。このようにサイバーと実際の空爆を組み合わせることで効果的な軍事作戦が実施できる。

また、2010 年、イランの核開発において濃縮ウランを作成するにあたってアフマディネジャドが遠心分離器を公開。しかし、その後遠心分離器 4 千本中、1 千本の回転スピードが狂い始めた。イランの技術者は当初原因が掴めなかったものの、システム上使用していた PC を自宅に持ち帰りインターネットに繋いだところそこからウイルスが拡散し東欧の技術者が当該 PC の感染を指摘。ウイルスは「STUXNET」と呼ばれ、米・イスラエルの共同攻撃ではないかと言われる。イランの核開発施設は外部のネットとは繋がっていなかったものの、何らかの方法で核開発施設にて使用されていたシーメンス社の制御システムのソフトウェアが狙われたとされる。

<u>サイバー戦争と作戦領域の変化</u>

- オバマ政権は 2012 年頃より政策を転換させ、「作戦領域の変化」を唱え始める。これまでは「陸・海・空」の 3 領域から、第 4、第 5 の領域として「宇宙」「サイバー」が加わり、米軍内に宇宙軍および、サイバー軍が設置され、サイバー軍（マイク・ロジャーズ司令官）は現在数千人規模となっている。
- ただし、新領域とされるサイバー・スペースは実態として空間的スペースを伴うものではなく、その実は各端末と回線の集積である。

<u>サイバー防衛の担い手</u>

- サイバー活動・防衛には geek と呼ばれるサイバーオタクを味方に使えることが欠かせない。世の中で一番有名な geek はエドワード・スノーデンだが、彼は米 NSA（国家安全保障局。国防総省の諜報機関。）に所属しサイバー領域で活動していた。
- ハワイの NSA（ダウンタウンより 1 時間ほどの距離にあり地下 5 階の施設）は、アジア太平洋のサイバー活動を監視（トラフィック・モニタリング）する拠点となっている。テキサスやジョージアなど地域別に分かれて大きな拠点が築かれている。それらで集めた情報をユタ州にあるデータセンターに一旦集積し、最終的にはメリーランド州にある NSA 本部に必要な情報を渡すこととなる。そこからホワイトハウス、ペンタゴン、CIA へと振り分けられる形となる。アトリビューション問題をトラックしているのも NSA である。ハワイには上記以外にも 2012 年 1 月に設置した新たな施設もある。

日本の対応

- 日本は、2013 年 6 月に「サイバーセキュリティ戦略」を打ち出し、情報セキュリティ会議（議長：官房長官）が中心になって対応していた。2014 年 3 月にサイバー防衛隊（90 名）を設置、11 月に「サイバー基本法」を可決した。これによって情報セキュリティ政策会議はサイバーセキュリティ戦略本部に改組された。陸・海・空自衛隊の通信担当員を合わせると計 2～300 名になる（米国の約 1/10 の規模、サイバー軍司令官のマイク・ロジャーズは四つ星の最高位の大将に対して日本のサイバー防衛隊の長は一佐)。
- 2015 年 6 月に新たなサイバーセキュリティ戦略を通そうとしたが、年金問題により延期・見直し状態となっている。また、東京オリンピックに向けてサイバー対策を急いでいる。ロンドンオリンピックの際には 2 億件のサイバー攻撃があったとも言われる。日本の当局者はイギリスの GCHQ（英国通信本部。オリンピック時に GCHQ は NSA からの情報提供を受けていた）にヒアリング等調査を行っている。
- 日本においては、伝統的に防衛省の情報本部が情報活動の中核を担ってきたがその中心となるのは無線通信傍受であり、有線通信の解析を主とする日本版 GCHQ も日本版 NSA もないために諸外国との情報交換・共有の機能性から行ってもカウンターパートの組織の立ち上げ等、対策が課題となっている。
- 2015 年 5 月に生じた日本年金機構の年金情報管理システムへの不正アクセスによる個人情報の流出は、情報の取得が目的ではなく日本政府へのネットワークへの侵入が最大の目的と考えるのが自然。情報を取得したが故に大問題となったため侵入した側としては失敗したと考えているはず。
- 2015 年 6 月、米国政府職員の人事情報を管理するシステムがサイバー攻撃を受け、約 400 万人分の個人情報等機密性の高い情報が流出した。米国側は攻撃元に中国が関係しているとし､6 月下旬に開かられた米中戦略対話でも大問題となった。7 月に入って流出数は 2200 万人に膨れ上がっている。中国の関与が疑われているが、それに対して、中国もまた反テロ法の一部としてサイバーセキュリティ法案を提出している。

中国の対応と今後の課題

- 中国は、2013 年 6 月の米中首脳会談後、中央インターネット及び情報化ワーキング・グループ（領導小組）を組織し、議長に習近平が就いた。2014 年に 1 回、2015 年に 1 回会合が開かれている。元々、中国では国家インターネット情報弁公室がサイバーに関して担当とされていたが、権限が弱く、領導小組ができたことによって弁公室がその管轄に入り、地位も向上し権限が強化され HQ として機能するようになった。

- 中国政府は情報制御について人民をコントロールすることから ISP のコントロールに切り替え効率化を図っている。ISP は免許制なので政府の指示に従わなければ免許が取り上げられることになる。それによって、ISP は自主規制を強化し、ユーザーを監視する方向に進んでいる。
- 中国人同士や外国から中国へのサイバー攻撃も激しくなっており、中国としては米国のサイバー攻撃能力との格差が開いて劣勢に立たされているとの現状認識から米国のできることは自らもできるようになりたいとの願望を多分にして抱えていると考えられる。この攻撃の応酬が米中間で激しくなり、米国側も我慢の限界に達しつつある。今後双方がどのように攻撃を抑制していくのかがポイントになる。
- 今後 9 月の国連総会において GGE（政府専門家会合）報告書の提出が見込まれる。国際法の適用において、日米豪欧は既存の国際法をサイバー・スペースにも適用するべきと主張し、中露・その他発展途上国は新条約が必要であり政府がその管理主体となるべきとの立場を取る。この裏には自国内の情報統制を国際条約によって正当化したい狙いや条約を作るプロセスを通じて米国主導の現状に対抗する狙いがある。米国等はインターネットでの表現の自由を前提にこれに反対している。
- サイバーセキュリティ対策としてインテリジェンス活動が不可欠となってきているが、日本において誰がこれをやるのかが問題となる。ソフトウェアへの対策だけでなく、ハードウェア、インフラの防衛も重要になる。

（2） 研究会ディスカッション

研究会のディスカッションでは、上記講演を踏まえて以下の点を中心に議論した。

- サイバーセキュリティにおける抑止と日米中関係の安定
- サイバー攻撃とテロ
- 中国とサイバー攻撃
- 世界のサイバー事情と日本のサイバー能力などの比較
- サイバー攻撃と日本の安全保障
- 平時でのサイバーセキュリティ
- サイバー問題と政府のコントロール／国際法の整備
- ハッカーの実態について
- サイバー防衛と今後の課題

（了）