S-H24-299

安心・安全社会の実現を阻むサイバー脅威の実態と対応策に関する国際的動向の調査研究

(財)ディフェンスリサーチセンター　　横山　恭三

1. 背景と目的

サイバー空間として知られる全地球的に相互に接続された情報・通信社会基盤は、近代社会のほぼ全ての活動の側面を支えるとともに、国家の経済、公共インフラ、市民の安全、及び国家安全保障に対して重要な基盤を提供している。このため、開放性、相互運用性、セキュリティ、及び信頼性を持った情報交換の媒体としてのインターネットを確保することは、国家のみならず国際社会の繁栄、安全保障の促進にとって不可欠なものとなっている。

しかし、デジタル社会の基盤設計の思想は、安全より相互運用性と効率性により重点が置かれている。結果的に、増大する国家主体や非国家主体のサイバー空間での活動家は、情報を漏洩、窃盗、変更、又は破壊し、情報システムに重大な混乱を引き起こすことができる。その実態は社会の混乱、金融被害、テロ活動の助長、安全保障上の諸問題等、広範多岐にわたるものであり、海外諸国においてもその対応に苦慮しているところである。

最近の世界的なサイバー攻撃の傾向としては、重要インフラに対する攻撃が激増している。この領域に対するサイバー攻撃は、国民の財産と生命を脅かす可能性がある。安全・安心なサイバー空間を構築することは我が国の喫緊の課題である。

本調査研究においては、サイバーセキュリティへの取組みが進んでいる欧米諸国の政策・戦略や取組みの実態、及びサイバー技術の国際標準やサイバー空間における国家の行動基準等を協議している国際機関等の動向を調査し、今後の我が国のサイバーセキュリティ体制の在り方の検討に資する情報を取りまとめることを目的とする。

2. サイバー空間の脅威の現状

(1) サーバー空間の脅威として、①コンピュータネットワークを通じた電子的攻撃（サイバー攻撃）、②電磁波による攻撃、③自然災害や事故による脅威、④部内者の怠慢と過失、⑤サプライチェーン攻撃、及び⑥インサイダー攻撃がある。この内サプライチェーン攻撃については、我が国ではサプライチェーン攻撃の重大性の認識が不十分であるが、米国や英国では、早くからサプライチェーン攻撃の可能性が認識されその対策が開発されている。

(2) サイバー攻撃の実行者として、①ハッカー、②インサイダー、③テロ組織、④ハクティビスト、⑤サイバーマフィア、⑥外国の諜報機関、及び⑦軍隊のサイバー部隊が存在する。サイバー空間は、陸、海、空、宇宙に次ぐ第５番目の戦場になったと言われる

ように、現在、外国の諜報機関やサイバー部隊によるサイバー空間での諜報活動（情報窃取）の活発化が指摘されている。

(3) 最近のサイバー攻撃の世界的な傾向として、重要インフラに対する攻撃が激増している。重要インフラの攻撃とは、その制御システム（SCADA）を狙ったものである。一般に産業用システムはサイバー攻撃を避けるため、インターネットなどの危険なネットワークから物理的に切り離されている。しかし、スタックスネット（Stuxnet）の例でも分かるように、重要システムが外のシステムに接続されなくても、インサイダー等によりシステムに直接マルウエアが挿入される可能性はなくならない。今後も、重要インフラに対する攻撃が増加すると予想される。

3. サイバー脅威に対応する国際的な枠組み及び我が国の関与

各国は、サイバー空間の保護やサイバー攻撃への対処において、国と国との間におけるサイバー関連情報の共有が不可欠であるとの認識で一致し、現在、国境を越えたサイバー空間における各種脅威に対処するためのインシデント情報の作成・共有、技術の国際標準化、法執行機関の連携、国家の行動規範の確立などの議論が各種の国際的な枠組みで行われている。その枠組みには、国際電気通信連合（ITU)、インターネット・ガバナンス・フォーラム（IGF)、ICANN、メリデイアン・カンファレンス、国際監視警戒ネットワーク（IWWN)、FIRST、アジア太平洋コンピュータ緊急対応チーム（APCERT）などがある。しかし、国際協調の裏にはインターネットガバナンスを巡る対立も存在する。米国をはじめとする西側民主国家はサイバー空間における表現の自由やプライバシーは尊重されなければならないと主張するが他方、中国、ロシアなどの独裁国家やイラクなどのイスラム国家は、インターネットの使用を規制するなど国家の管理を強化しようとしている。このような問題の背景には、インターネットガバナンスを含むサイバー空間における国際規範が未だ確立していないことがある。今後、我が国もサイバー空間のルール作りに積極的に参加すべきである。

4. サイバー脅威に対応するEU及び主要国の取組み

各国ともサイバー戦略を策定し、目標と具体的施策を明示している。おおよそ各国とも、目標として、①準備と防止、②探知と対応、③軽減と回復、及び④国際協力、を掲げ、具体的な施策としては、①24時間体制でサイバー脅威を監視する組織（CERT）の設置、②政府全体に対し統一的かつ横断的なサイバー攻撃対策を推進する政府機関の設置、③国民の認識向上のための啓蒙・教育、④重要インフラ防護のための公共機関及び企業との連携、⑤ITセキュリティの標準化及び犯罪取締りのための国際協力、及び⑥熟練したサイバーセキュリティ要員の発掘・育成を掲げている。

特に、米国のサイバーセキュリティ政策の経緯を見ると、2008 年以降 1 年おきに戦略等を策定・発出している。これは、サイバー空間おいては、攻撃ウイルスが出現してから防御側がアンチウイルスソフトを開発するなど攻撃側が圧倒的に有利であるため、なかなか対策の成果が得られていないことを示している。このような中、米国は、「サイバー空間のための国際戦略」の中で、サイバー攻撃に対して必要に応じてかつ適用される国際法に基づき、軍事力を含むあらゆる手段で対応することを宣言した。

5. 我が国の情報セキュリティ対策への取組み

日本の情報セキュリティ対策は、サイバー犯罪及びサイバーテロへの対応からスタートしたが、現在は災害による ICT 障害への対応も含めた総合的な対策へと変化している。今日、最優先されるべき脅威はサイバーテロである。然るに、我が国の最新の情報セキュリティ戦略である「国民を守る情報セキュリティ戦略」は総花的であり、政府の責任として重要インフラ防護が強調されていないことはゆゆしき問題である。

6. 我が国の国情、国民性に適した今後の対応策（提言）

(1) 国家 CERT の設立

国内外にアピールできる権威ある国家 CERT を設立する。

(2) 国家重要インフラ防護センターの設立

現在、我が国に欠落している国家重要インフラ防護センターを設立する。

(3) 情報セキュリティに関する資格制度の導入

国として資格制度を確立し、官民を相互に経験できるキャリアーパスを形成する。

(4) 天才ハッカーの発掘

若き天才ハッカーを発掘するためのハッカー大会を国が開催又は支援する。

(5) サプライチェーン攻撃対処への取組み

官民のサプライチェーン攻撃に対する認識を向上する。

(6) 犯罪捜査のための通信傍受要件の緩和

「犯罪捜査のための通信傍受に関する法律」の通信傍受の要件を緩和する。

(7) サイバーテロに対する制裁的抑止力の開発・保持

ウイルス・アンチウイルスを開発する国立の研究所を設立する。（了）

7. 謝辞

本調査研究は、（財）新技術振興渡辺記念会より、平成 24 年度上期の科学技術調査研究助成を受けて、平成 24 年 4 月より平成 25 年 3 月までの間、（財）ディフェンス リサーチ センターが実施したものである。関係各位に深甚なる謝意を表する。