平和研所内会議

2011 年 10 月 24 日(月) 開催

テーマ:「サイバー空間における安全保障上の諸問題:新たな局面に入るサイバー戦争」

報告者:大澤 淳(主任研究員)

概要

1 2011年は、我が国政府機関へのサイバー攻撃が相次いで明らかになった年であった。1月に経済産業省への標的型攻撃が明らかになったのをはじめ、9月には三菱重工等の防衛関連産業への攻撃が報道された。さらに、10月には、衆議院のコンピュータ・ネットワークへの攻撃が報道され、サーバー等数十台が攻撃によって感染させられたことが判明した。このような政府機関を狙った標的型攻撃は、すでに2007年頃より行われていたと見られるが、今年に入って被害の様子が報道され、広く世間に知られるようになった。サイバー攻撃の現状が広く認知されるようになった点で、2011年は「サイバー戦争元年」とも言うことができよう。

2 最近のサイバー攻撃における状況の変化として、①重要情報の窃取を狙う標的型攻撃への移行、②制御システムを狙ったサイバー攻撃の本格化、を指摘することができる。

2.1 ①重要情報の窃取を狙う標的型攻撃

2007年頃より、サイバー攻撃は、不特定多数への感染を意図した愉快犯的なものから、特定の組織・個人から機密情報を窃取することを目的とした標的型攻撃へと変わってきている。

最近、我が国の議会・政府機関・防衛産業などを狙った攻撃が相次いで発覚しており、国全体をあげた対策が急務である。

2.2 ②制御システムを狙った攻撃

近年、標的型攻撃だけでなく、社会の重要インフラの制御を麻痺させることを目的とした攻撃の前兆が見られるようになっている。制御システムへの攻撃は、実際の人命にも関わる問題として、米国等ではサイバー領域の優先課題となってきている。

電力・ガス等の国の基幹となる重要インフラをはじめ、あらゆる産業にわたる制御システムを国全体をあげてサイバー攻撃から防護することが喫緊の課題である。

3 特に後者の制御システムを狙った攻撃として昨年情報セキュリティ関係者の注目を集めたのは、イランの核施設の制御機器をターゲットにしたと見られる「Stuxnet」であった。「Stuxnet」を詳細に分析した大手セキュリティ会社シマンテック社の関係者は、「Stuxnet」

は、この20年間で最も重大なセキュリティ上の出来事であり、物理施設を実際に攻撃した初めてのマルウェアであった、と指摘している。「Stuxnet」は、１５の異なるモジュールで動作しており、複数の技術者が数ヶ月から数年かけて開発に関わったと分析されており、インターネットに接続されていないウラン濃縮用遠心分離器を制御する高周波コンバーターの制御を乗っ取るまでに、2年以上の歳月をかけていることから、国家レベルのサイバー攻撃モジュールである事が指摘されている。

4　米国などでは、２０００年以降、ガスや電気、水道といった社会の重要インフラの制御を麻痺させることを目的とした攻撃の前兆が見られるようになっている。電力・ガス等の重要インフラが依存する産業用の制御システムはPLC(プログラマブル・ロジック・コントローラ）やアクチュエーター、バルブ制御装置などのフィールド制御機器および状況の監視・計測に用いられるサーバーやクライアントPCなど一群の情報機器群から成り立っている。本来制御システムは、常時ネットワークに接続されていないか、ファイアウォールを介してネットワークにつなげる等のセキュリティ措置が取られているため、サイバー攻撃の影響を受けにくいと言われてきた。また、事業者ごとにカスタマイズされた固有のシステムが使われているため、システム内部を熟知しなければ攻撃は難しく、一般的なコンピュータ・ウィルスの影響も受けないと考えられてきた。しかし、実際のところ、そのような制御システムもPCなどと同じOSを利用しているケースが多く、外部からの情報入力も定期的に行われているため、サイバー攻撃を受ける危険性が高いことが最近明らかになってきている。

5　米国大統領情報問題担当補佐官であったリチャード・クラークは、著書の中で、「サイバー戦争は現実であり」「すでにはじまっている」と指摘し、サイバー戦争は「世界の軍事バランスや政治経済の関係を根底から覆す恐れ」があると述べている。実際、サイバー戦争を見据えた各国の取り組みはすでにはじまっており、中国では、サイバー戦争を意味する「超限戦」の考え方が1999年にすでに提唱され、2002年頃から、人民解放軍は各軍管区傘下部隊に、情報戦民兵組織を設置し、民間のIT企業、大学、人民解放軍のコンピュータ・ネットワーク作戦部隊の人間からなる混成部隊を編成している。北朝鮮でも、小学生の時から選抜・養成されたサイバー戦闘員からなるサイバー部隊が数千名いるとされている。米国では、サイバー戦争の危機感の高まりを受け、「サイバーコマンド（情報戦総司令部）」が設置され、陸海空海兵の4軍に「陸軍サイバー司令部」「第24空軍」「第10艦隊」「海兵隊サイバー司令部」が編成されている。諸外国に比べ、我が国のサイバー空間を守る取り組みは遅れていると言わざるを得ない。

6　我が国のサーバー空間を守るにあたっては、①攻撃をいち早く察知し、早期警戒を周知徹底することが必須であり、三権分立や官民を問わず、国全体を包摂して攻撃情報の

収集・分析にあたる組織が必要である。また、②攻撃パターンを収集・分析し、攻撃に対処し、重要インフラを防護するための実働部隊の編成も必要となる。さらに、③サイバー戦争を勝ち抜く人材の育成も欠かすことができない。

7　サイバー攻撃は防衛だけでは完全に防御できない。攻撃元のネットワークに逆侵入し、相手方の特定や反撃を行うような「自衛的なサイバー反撃」を容認することも必要である。

以上