サイバーアタック

情報ネットワークに潜むリスク

2013 年 5 月 2 日、オーストリア、ウィーンの送電コントロールセンター・E-Control 管轄下の電力消費量が、異常急上昇。自動データコントロールが効かなくなった。最初は、発電所の部品欠陥かと調査したが、原因不明で、Black-out 寸前の危機に遭遇。プログラムをマニュアル操作できるスペシャリストがいるのが幸いし、原因究明、手動で正常化。原因は、提携先のドイツのガス会社のオペレーションプログラム。特に、悪意のあるハッカー、IT テロではなかったが、ちょっとしたプログラムのパラメータの波及効果の見落としで、大変なパニック状態に陥るところを未然に防いでいる。

2015 年 1 月半ば、ドイツのテレビ ARD は、米国家安全保障局（NSA, The National Security Agency）が極秘に大量の個人情報を収集していたことを、米中央情報局（CIA）元職員 Edward Joseph Snowden（エドワード・スノーデン　写真下）が告発した「スノーデン事件」のドキュメンタリーを放映。欧州の公機関、高度のノウハウを持つ企業、エネルギー拠点が、いかに被害をこうむっているか、その現状とインターネットに潜むリスクをルポ。

莫大な予算がついている米国の NSA のトップからの指令・サイバーコマンド（Cybercommand）は、欧州のテレコミュニケーションネットワークの独占を狙っている。また、世界各国の石油ガスの供給ライン、交通機関システムのオペレーションシステムも NSA の標的。イラン Natanz にあるプルトニウム精錬プラントを攻撃したコンピュータウイルス Stuxnet は、米国が仕掛けている。Mahumud Ahmadinedschad（マフムード・アフマディーネジャード）が訪問しての 2010 年 4 月 8 日の同プラント竣工式の際、コンピュータウィルス Stuxnet により、60 ある遠心機が機能しなかった。米国は、長年イランをスパイ。その予算は、軍事予算なみの約 50mil US$ （Yen 5,906,500,000）で、米国内にイランの Natanz 基地とまったく同様の施設まで作って、攻撃のタイミングを狙っていた。この日、個々の遠心機が異常回転、部品が異常回転で消耗し物理的に故障。この被害は、イラン国内のみでなく、技術提供していた、ドイツ Siemens(シーメンス)社の BBXI Software Manipulation も感染。（この苦い経験をもとに、ドイツでは、Stuxnet を逆手に取り、解析。今後のサイバーアタックに備える体制に入っている。）

2012 年 4 月 10 日には、今度は、イランからの逆襲。ニューヨークの株式市場のサーバーをアタック。イランは、まず、ドイツのサーバーのアルゴリズムを破壊することを通して、ニューヨークに被害をあたえた。この際、最初に犯行を疑われたのは、ドイツのサーバー。一時的に米独の関係が悪化したことは言うまでもない。

さらに、Snowden によると、NSA は、EU コミッション、そして意外にも NATO のテレコミュニケーション、Belgacom を英国

の GCHQ（The Gouvernement Communications Headquarters 政府通信本部イギリスの情報共同体において、偵察衛星や電子機器を用いた国内外の情報収集・暗号解読業務を担当する諜報機関）を通してスパイ。同システム機能にサボタージュを組み込んでおり、EU 議会議員の携帯電話も、盗聴されている。もちろん、EU 側は、対応策を設置してはいるが、このほかに、海底ケーブル、通信用人工衛星も、NSA は、盗聴。現在稼動しているコンピュータシステムのうち 70,000 件も盗聴、また、ウイルスを潜ませ、何かの拍子にシステムが感染するようにしてしまっている。インターネット内に潜む地雷 Stuxnet、そこから派生したトロイの木馬型マルウェアであるドゥークー（英語版）やフレイム（英語版）は、米国内では、Pentagon にも、被害をおよぼしている。Snowden いわく、防衛等国家レベル、企業の決断をコンピュータのソフトウェアーのみに頼るべきではない！

現在、欧州では、企業・インフラストラクチャー等、重要な約 56,000 のオペレーションシステムが、特にパスワードもなく機能している。それをスパイしたり、コンピュータウィルスを潜ませ、システム機能のサポタージュ、あるいは、データを盗用、変更してしまうことは、ハッカーにとっては、意外に簡単。

大学病院、発電所等の一般市民の厚生保持、産業交通インフラ基盤、各企業の独自の技術情報セキュリティーに支障が起きることは、どんなことがあっても避けなければならない。

高度のノウハウをもつドイツの化学・工作機械、自動車業界、そのサプライヤーも、産業スパイの格好のターゲットとなっている昨今、ドイツでは、Hamburg（ハンブルグ）に約 800 名の IT 専門家を置き、産業のネットワーク化を進める“Industrie 4.0“などの情報安全の監視を推進している。

National IT Summit で“Industrie 4.0“の情報安全についてスピーチするメルケル首相 21. Oktober 2014 in Hamburg

また、Bonn（ボン）の Godesberg（ゴーデスベルグ）に、連邦情報技術保安機関（写真下 BSI Bundesamt für Sicherheit in der Informationstechnik）をおき、政府はじめ公共のサーバーの安全性保持に取り組んでいる。危険な要因を 5 分間以内に察知し、発信もとを探知することなどに挑戦。また、各企業にも IT Security にもっと予算を取ることを呼びかけている。しかし、高額のため、企業側からの動きがなかなか見られないところが、落とし穴。米国 NSA のみならず、ロシア、中国からのサイバーアタックは、今後も続くだろう。（日々、悪化しているロシア・ウクライナ抗争で、ウクライナからの外交団がベルリンを訪問した際、ドイツ連邦議員たちが使用しているメールサーバーが、ロシアからのウィルスで一時遮断。）今までにはなかった、情報ネットワークに潜むリスクへの対策は、今後の大きな課題である。

26.01.2015　小澤エネルギー研究所
Setsuko Schwarzer

Information Source：
http://www.ardmediathek.de/tv/Reportage-Dokumentation/Die-Story-im-Ersten-Schlachtfeld-Intern/Das-Erste/Video?documentId=25812360&bcastId=799280&mpage=page.info
http://en.wikipedia.org/wiki/Government_Communications_Headquarters