原子力の平和利用に向けた取組（9）
～核セキュリティ・サイバーテロの脅威～

日本核物質管理学会事務局長・岩本友則

（サイバー戦争の幕開け）

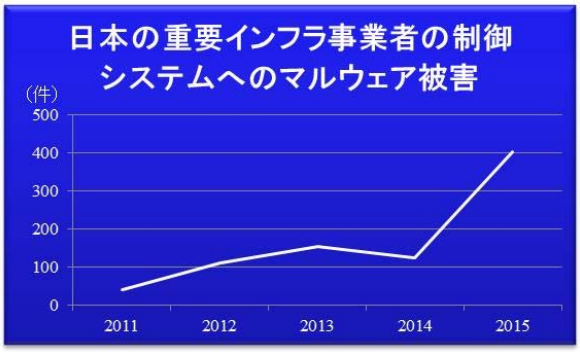
日々進歩するIT技術、原子力施設の核セキュリティにおいて、プラント制御システムに対するサイバー攻撃対策が最も重要かつ急務と言えます。

2010年11月、「Stuxnet（スタックスネット）」と呼ばれるコンピュータウイルスを用いたサイバー攻撃によりイランのナタンズ濃縮工場の遠心分離機約8400台が破壊されると言う物理的被害が発生しました。当該濃縮工場の運転制御システムは、外部のインターネットには接続されておらず完全に隔離されていましたが、インターネットに接続しているパソコンからUSBメモリーを介してプラント運転制御システムに感染したものでした。このスタックスネットは、ナタンズ濃縮工場の運転操作員には、システムが正常に運転していると見せかけて遠心分離機を破壊に至らしめていたのです。この事象は、ある国の関与が垣間見られることから国家間サイバー戦争の幕開けとも言われ、また、これまでのサイバーセキュリティの基本概念「①制御システムはサイバー攻撃とは無縁、②制御システムをインターネットと切り離しておけば大丈夫、制御システムは、特殊な構成だから外部の者に分かるはずがない、新品のUSBメモリだけを使えば安全、マルウェアに感染するとコンピュータの動きが異常になる。」を完全に打ち破ったのです。

写真は、**Presidency of The Islamic Republic of Iran** http://www.president.ir/en/ Tuesday 08 April 2008 より

（拡大する被害）

コンピュータシステム防護の要として、ファイヤーウオールが用いられてきましたが、今や有効な手段とは言えなくなりました。その実態として日本の重要インフラ(電気、水道、ガス等)事業者の制御システムに対するマルウェア被害は、2011年の約50件に対し2015年では約400件と上昇しています(グラフ参照)



海外でも2012年サウジアラビアの国営石油会社への攻撃で、3万台のパソコン破壊、2014年ドイツの製鉄所への攻撃で操業停止、更に2015年ウクライナ電力施設へのサイバー攻撃で複数の電力供給会社に対しマルウェアを使用した攻撃が仕掛けられ、このうち1社はITシステムに不正侵入され、約8万人の顧客の電力供給に支障が生じ、かつ同時に電話回線への障害が発生しています。

新種のマルウェア発生数も2011年の約60件に対し2016年では10倍に増加しています。今やサイバー攻撃は特別なものではなく、攻撃ツールがインターネット上に出回り誰もが容易にサイバー攻撃を行う事が出来る環境が整っているばかりか、新たに作ったマルウェアが既存のアンチウイルスソフトに探知されるか否か確認する闇サイトまで存在しています。

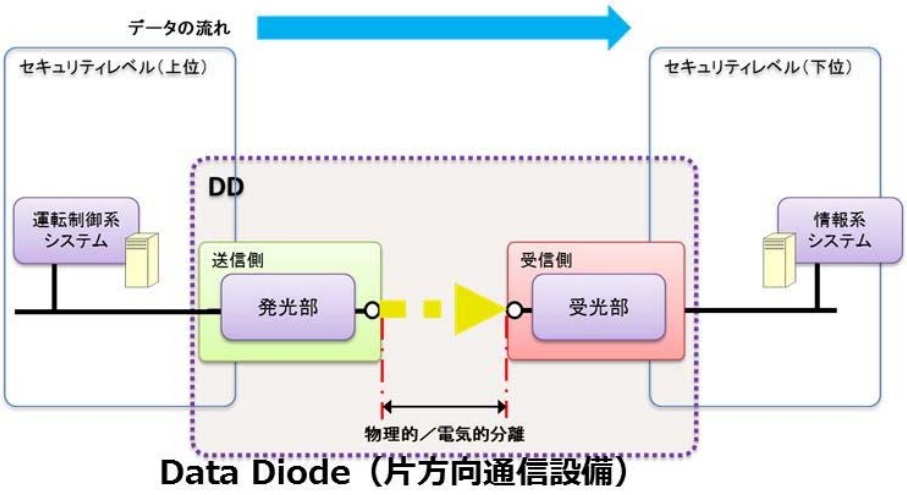
従って、インターネットに接続されているコンピュータが攻撃対象となった場合、残念なことに防御出来ません。

原子力施設でサイバー攻撃を受けた場合、①機微情報の漏洩、②核物質等の放出、③機器の異常／破壊、④工場の停止、⑤端末の破壊・故障等の深刻な事態を招くことになります。従って、原子力施設はサイバー攻撃に対する堅固な防護システムの整備が不可欠です。

（サイバーテロへの対応）

こうしたサイバー攻撃の脅威に対処するため国際原子力機関（IAEA）は、ガイドラインとして「原子力発電所等におけるコンピュータセキュリティ」を定め各国のサイバーセキュリティの強化を図っています。先行している米国では、業界規格が整備されており業界で標準化が図られています。一方、我が国においても 2018 年 3 月 1 日に原子力規制庁に「サイバーセキュリティ対策チーム」が設置され我が国の原子力施設に対するサイバーセキュリティ対策の強化を図ると共に、サイバーセキュリティに精通した人材の確保と育成を進めています。

プラント制御システムのサイバーセキュリティ対策として、第１に、プラント制御系コンピュータシステムについて外部システムと電気的、物理的隔離の実施です。この技術的ツールとして、片方通信設備（Data Diode=データダイオード）を設置します。これは、図に示すように光の発光部と受光部によりデータの片方向送信を可能とします。第２に、プラント制御システムの更新、メンテナンス等に用いるパソコン（PC）や USB メモリ、CD/DVD 等の記憶媒体は、作業前のウイルスチェック実施、によるマルウェアの確認をします。第３に、プラント制御に係るプログラミングされたシステム及び記憶媒体接続ポート等設置制御盤に対する施錠等のアクセス管理に加え、内部脅威低減のため２人以上での作業の実施（相互監視）です。更に上記に加えて、サイバーセキュリティに係る教育・訓練とサイバー攻撃事象に対する対策組織の設置です。



Data Diode（片方向通信設備）

多様化するサイバー攻撃に対する訓練は、非常に難しいのが現状ですが、宮城県多賀城市に技術研究組合「制御システムセキュリティセンター」が設置されており、ここでは、重要インフラに対するサイバーセキュリティの最前線と各種サイバー攻撃を模擬した対応訓練が実施されています。また、原子力施設の制御システムを模擬したサイバー攻撃訓練のサービスを提供している大手企業もあり、この様な努力を通して、日本の原子力施設におけるサイバーセキュリティ対策は、確実に向上しているのです。

マルウェアとは、ウイルス（PC などの端末の故障・障害を引き起こす）やスパイウェア（個人情報流出などの原因）、ワーム（自己複製能力を持ち悪影響を及ぼす）など悪意をもって動作するようプログラムされたソフトウェアを総称したものです。