交流のひろば/agora ―*crosstalking*―

世界の産業インフラに対するサイバー攻撃とセキュリティ対策の実情

佐々木　弘　志

「サイバー攻撃」の対象は，今や，情報システムだけではなく，産業インフラのシステムにまで広がっている。世界中で，産業インフラを標的としたサイバー攻撃が発生する中で，特に，東京オリンピック・パラリンピックを2020年に控えた日本では，今後のインフラ整備において，サイバーセキュリティの観点は不可欠とされている。本記事では，産業インフラに迫るサイバー攻撃とはどういうものかを，その危険性や実態を踏まえて紹介したあと，世界および国内におけるセキュリティ対策の最新トレンドについて概観する。

キーワード：産業インフラ，サイバーセキュリティ，多層防御，状況認識，テロ対策

1. 産業インフラへのサイバー攻撃は第５の戦場

皆さんは，「サイバー攻撃」と聞いて，どのような攻撃を思い浮かべるだろうか？　近年では，年金機構の情報漏えいなど，メディアを騒がせる事件が頻発しており，サイバー攻撃そのものは身近に感じられるようになってきたのではないか。皆さんが思い浮かべる攻撃はというと，おそらく，「他国の犯罪組織などが，特定の組織（企業，政府等）を狙い，インターネットを介して，個人情報等の機密情報を窃取したりすること」が最も多いのではないかと予想される。実際，その認識は正しいのだが，実はこの攻撃に加えて，ここ数年，いわゆる産業インフラのシステムに対するサイバー攻撃が顕在化してきた。まだ，公知となっている攻撃数としては多くはないが，その攻撃は着実に進化してきており，世界的な課題となっている。ここでいう産業インフラとは，電力，ガス，水道，プラント（化学，金属等），金融，ロジスティクス（輸送）など産業を支えるために必要な基盤のことを指す。まず，産業インフラにおけるサイバー攻撃の特徴は何かについて説明していこう。

最初に大きな特徴として挙げられるのは，攻撃の目的である。例えば，情報システムを狙った通常のサイバー攻撃の特徴として，「見つからないように情報を窃取する」ことがあげられるだろう。すなわち，この場合のサイバー攻撃者の最終目的は「情報の窃取」であり，それを行ったことさえも見つからないことが望ましいとされる。ところが，Stuxnet（スタクスネット）[a)]等で知られる産業インフラを標的としたサイバー攻撃は，「最終的に破壊する」ことを目的とする場合があるという特徴をもっている。このような目的のもとに攻撃が行われる背景には，サイバー空間が，陸，海，空，宇宙に続く，「第５の戦場」として捉えられているという事情がある。つまり，戦争行為の手段としてのサイバー攻撃が注目される中で，相手国に効果的にダメージを与える標的として，産業インフラが注目されているということだ。実際に，2015年の12月23日にウクライナ西部で大規模な停電を引き起こしたサイバー攻撃は，ロシアの組織の関与が疑われており，まさに，国家間の紛争における攻撃の手段として，産業インフラを標的としたサイバー攻撃が行われていることの具体例といえる。

では，なぜ，最近になって産業インフラに対するサイバー攻撃の危険性が高まっているのだろうか。もちろん攻撃側のツールの進歩も挙げられるのだが，産業インフラならではの事情も存在する。

産業インフラを支えるシステムとして，「制御システム」と呼ばれるシステムが存在する。これらは産業インフラの性質上，基本的に停止することなく稼動すること（可用性）が求められる。また，システムの寿命も十年単位というものがほとんどで，古いシステムが残り続けるという事情がある。これまでの制御シス

a)：Stuxnet（スタクスネット）
産業用制御システムを攻撃する最初のマルウェアとして知られている。イランの核施設にある遠心分離機を破壊するために作成されたマルウェアと言われている。

テムは，外部との接続がされておらず，システムをコントロールするOSも制御システム専用であったため，いわゆる「クローズド」な環境にあり，一般のマルウェアとは無縁の存在であると信じられてきた。ところが，IT技術の進歩に伴い，工場やプラントのネットワーク化が進み，制御システムに汎用OSが採用される機会が増えてくるといった状況の中で，これまで「クローズド」だった制御システムが「オープン」になってしまい，攻撃者に必要とされる技術が彼らの得意分野と重なることで攻撃がしやすい状況が生まれてしまったのだ。

このようなオープン化の流れの中でも，制御システムは「可用性」により装置の交換や変更が簡単にできないため，脆弱性[b)]をもった古いシステムは依然として残り続けている。つまり，弱点はあるのに防御が簡単でないという状況が起こっているのだ。

2. 産業インフラへのサイバー攻撃の実態

次に，ここ数年，世界で実際に起こっている産業インフラに対するサイバー攻撃の例をいくつか紹介する。

以下に，産業インフラそのものに対する意図的な攻撃の可能性があるものだけを抽出した。したがって，偶発的なマルウェア感染の疑いが強いものや，産業インフラの攻撃を目的とした情報窃取の事例などは含んでいない。

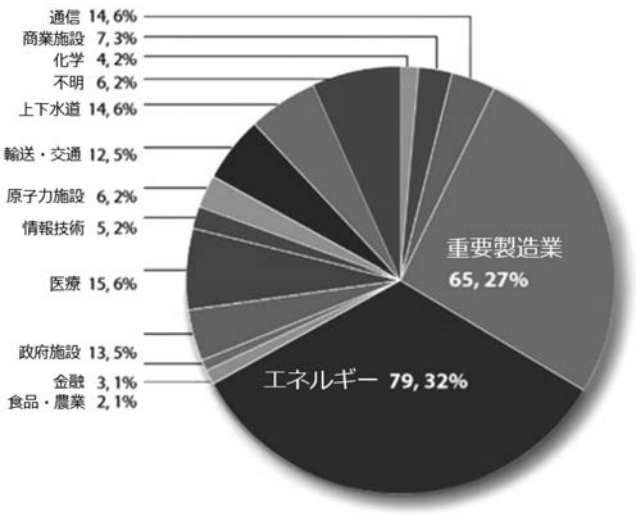
・2015年12月　ウクライナ西部にて，サイバー攻撃による大規模な停電が発生。
　ウクライナ政府がロシアの組織による犯行であるとの声明を発表。真偽は不明。
　大規模停電の原因がサイバー攻撃であると政府が認めた世界初の事例。
・2014年　ドイツの鉄鋼所がサイバー攻撃を受け溶鉱炉停止（具体的な場所は公開されていない）。
　ドイツ政府の情報セキュリティ庁（BSI）が2014年のレポートで公表
・2013年～2014年　複数の電力会社より，電力システムの管理サーバーの情報が外部に漏えい。
　一連の攻撃は「Operation Dragonfly」と呼ばれている。
・2013年3月　韓国政府機関，金融機関，メディアがサイバー攻撃を受け一時機能停止。
・2012年8月　サウジアラビアの石油会社で30,000台にのぼるワークステーションがサイバー攻撃を受けた。
　一連の攻撃は「Shamoon」と呼ばれている。
・2012年5月　米国ミシガン州の天然ガスパイプラインがサイバー攻撃を受けた。
・2011年2月　ブラジルの発電所で制御システムがマルウェアに感染し，運用停止（故意であるかどうかは不明）。
　（※ブラジルでは，2007年，2005年にもサイバー攻撃で停電が発生したといわれているが真偽は不明。）
・2009年～2010年　イランの核施設にある相当数の遠心分離機がマルウェアにより破壊された（Stuxnet）。

いずれも，大きな損害を生んでいるか，生む可能性の高いものであり，産業インフラに対するサイバー攻撃が行われた場合の影響の大きさを示しているといえる。

これらの事例に加えて，産業インフラにおけるサイバー攻撃の実態を示している統計を紹介する。

米国のICS-CERT（米国土安全保障省の産業制御システムセキュリティ機関）が2015年発表したレポートによれば，米国内の重要な産業インフラに対する攻撃が，2014年の1年間で，計245件報告されている。その対象となった産業の内訳は，エネルギー分野が32%を占め，続いて重要製造業分野（鉄，金属，発電，輸送部品などの製造）が27%で続いている（**図―1**参照）。

また，産業インフラへのサイバー攻撃の直接的な例



図―1　ICS-CERTの2015年発行のレポート「Year in Review 2014」より，サイバー攻撃によるインシデントが報告された重要な産業インフラ分野の内訳
（凡例：分野名，インシデント件数，全体における比率（%））

b)：脆弱性
　攻撃に悪用可能なシステム上の欠陥や仕様上の問題点のこと。

ではないが，潜在的な脅威の一例として，検索エンジン SHODAN の存在をあげておく。検索エンジン SHODAN は，インターネット接続している機器の情報を取得できる検索エンジンであり，遠隔監視システム，監視カメラ，プリンターに至るまでインターネット接続している機器に関する情報が確認できる（**図**―2 参照）。例えば，この検索エンジンを用いて，脆弱性の存在する古いバージョンのサーバソフトウェアを使っている設備を探し出し，その脆弱性を利用した攻撃を行うといった攻撃シナリオが考えられる。産業インフラのシステムは，前述のように古いシステムが残っているにも関わらず，対策もなしにインターネットに接続するなど，「オープン」になっている場合が多いため，このような攻撃の対象となりやすい。

図―2　検索エンジン SHODAN

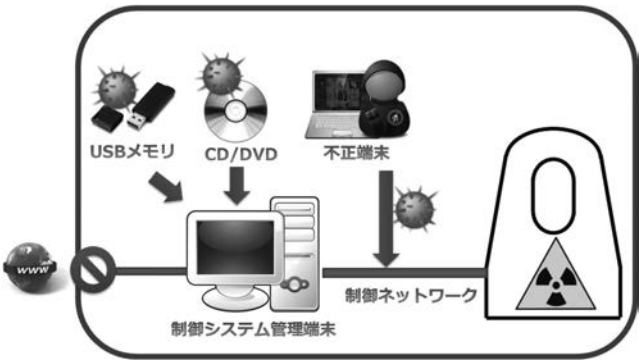
3. 産業インフラへのサイバー攻撃の手法

では，次に，産業インフラへのサイバー攻撃はどのような手法で行われるのかを実際の例を通して紹介する。

ここでは，産業用制御システムを攻撃した最初のマルウェア[c)]である Stuxnet の攻撃手法について紹介する。

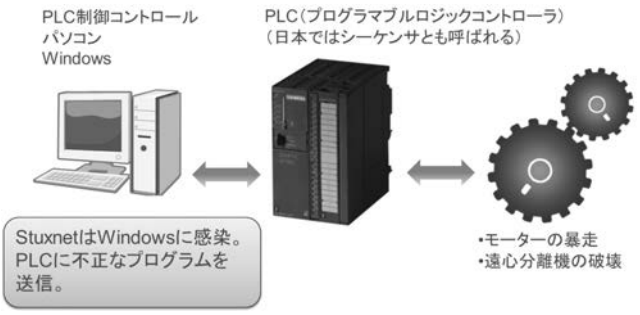
Stuxnet は，イランの核施設にある遠心分離機を破壊するために作成されたといわれるマルウェアである。ここでは産業インフラへのサイバー攻撃という観点でその攻撃手法について説明したい。

Stuxnet の一つ目の特徴は，その感染経路である。Stuxnet のイランの核施設における制御システムへの感染経路はデータのやり取りに使っていた USB メモリ経由であったといわれている。これは，産業インフラをコントロールする制御システムが仮に「クローズド」であって，外部から隔離されていたとしても，USB メモリ等のメディア経由でサイバー攻撃を受けることがあるという実例となったという点で大きな教訓を含んでいる（**図**―3 参照）。



図―3　Stuxnet に見られるクローズな環境に対する感染経路の例

また，二つ目の特徴は，その感染対象である。Stuxnet は，独シーメンス社の PLC（Programmable Logic Controller[d)]）を含むシステムを標的として設計されたマルウェアであり，シーメンス社の PLC のシステム以外では発動しないものである。しかし，このマルウェアは，PLC という制御システム専用 OS で動作する制御機器をハッキングしたわけではない。このマルウェアがハッキングしたのは，シーメンス社の PLC が動作するためのプログラムを作成，変更する目的をもったプログラミングツールと，PLC の状態を監視するモニタリングツールであり，ともに Windows OS で動作するアプリケーションである（**図**―4 参照）。つまり，あくまで対象アプリケーションが制御システムに関係するものであっただけで，そこに用いられている技術は，いわゆる従来のマルウェア作成の延長上にあるものだと考えられる。もちろん，制御システムに関する十分な知識が必要となるため，マルウェア開発が容易ではないという事情はあるものの，制御システムのオープン化に伴い攻撃のハードル



図―4　Stuxnet の感染対象は Windows

c)：マルウェア（malware）：
不正かつ有害な動作を行う意図で作成された，悪意のあるソフトウェアや悪質なコードの総称。いわゆる，コンピュータウイルスも含まれるが，マルウェアは，ワームやスパイウェア等，他の悪質なソフトウェアも含むため，コンピュータウイルスの代わりに広く使われるようになった。malicious software（悪意あるソフトウェア）の「mal」と「ware」を合わせた造語。

d)：PLC（Programmable Logic Controller）
プログラマブルロジックコントローラ。国内ではシーケンサとも呼ばれる。 小型のコンピュータの一種。ユーザが PLC 専用のプログラムを作成し，PLC に転送することで，さまざまな制御を行うことができる。

が下がっているといえる。

以上，Stuxnet の攻撃手法からわかることは，産業インフラをコントロールする制御システムがクローズドであったとしても，USB メモリなどの手段を用いて攻撃が可能であること，また，制御システム専用 OS を用いている制御システムそのものではなく，それを管理している汎用 OS のパソコンをハッキングする方法もあるということである。この Stuxnet 登場により，これまで，制御システムは「クローズド」だから攻撃が困難とされてきた神話が崩壊し，世界の攻撃者が産業インフラを新たな攻撃対象として認識したといえるだろう。

その証拠に，Stuxnet 以降，産業インフラを支える制御システムの脆弱性が次々と明らかになっている。ICS-CERT によれば，2010 年には 20 件だった制御システムの脆弱性報告が，2014 年には 159 件に増加している。これらの脆弱性報告には日本のベンダーのものも含まれている。今後は，情報システムと同様，このような脆弱性を利用したサイバー攻撃が増えていくものと考えられる。

4. 産業インフラへのサイバー攻撃に対する各国の危機意識と備え

ここまで，産業インフラへのサイバー攻撃の脅威について，さまざまな角度から紹介してきた。では，このような脅威に対して，世界各国はどのような対策を行っているのだろうか？

2013 年 2 月，米国のオバマ大統領が米国内の重要な産業インフラに対するサイバーセキュリティ強化策の大統領令に署名を行った。目的は，近年増加する重要な産業インフラに対するサイバー攻撃を未然に防ぐためである。この大統領令に基づいて，NIST Framework と呼ばれるセキュリティ対策のガイドラインが公開され，重要な産業インフラ事業者への対応が奨励されている。また，欧州においても，2015 年 12 月に EU（欧州連合）において，「NIS Directive（Network and Information Security Directive）」と呼ばれる情報セキュリティに関する指令（EU の各加盟国における法律化を求める強制力がある）の内容についての合意がなされた。この指令によると，加盟国において，必要不可欠なサービスを提供する，エネルギー，輸送，金融，医療分野，および，クラウドコンピューティングやサーチエンジンのような重要なデジタルサービスを提供する事業者は，適切なセキュリティ対策を行った上で，サイバーインシデントが発生した場合の国家機関への報告が求められることになる。

また，業界ごとに独自のセキュリティ対策を行っているケースもある。例えば，米国の電力業界が定めているセキュリティ対策の標準である NERC CIP がそれにあたる。NERC CIP とは，NERC[e] が策定した一定規模の発電設備と送電設備を有する電力インフラ事業者が順守しなければならないセキュリティ対策の規格であり，適用できていない事業者には罰金等のペナルティが科せられる。

これらの流れを受けて，日本国内でもガイドライン策定の動きが活発となってきた。例えば，電力自由化に向けて，新しい事業者の参入が想定される電力業界では，日本電気技術規格委員会（JESC）において，「電力制御システムセキュリティガイドライン」の策定が，2016 年 4 月の施行を目指して進められている。

いずれにせよ，世界の大きな潮流としては，国や業界主導で何らかのガイドラインなり規制を整備し，ある程度の強制力をもって，各事業者が何らかのセキュリティ対策を行うことを求めていくという方向だろう。

セキュリティ対策は，費用対効果が見えにくく，必要性が理解されない場合に対策がなされないということが容易に想像される中で，産業インフラ自体が攻撃対象になった場合の損害の大きさを考えると，国や業界がどこまでやったらいいかの基準を示しつつ，ある程度の強制力をもって進めざるをえないというのはごく自然な流れといえるだろう。

5. 具体的な対策例

では，具体的な対策例としてはどのようなものがあるのだろうか？　世界で行われている具体的な対策例として，最も厳しいレベルの基準に従っているといわれる米国の原子力発電所の例を紹介する。

9.11 のテロを経験した米国では，原子力施設のサイバーセキュリティは，テロ対策の一環として捉えられている。実際に，米国の原子力規制委員会[f] は，原発事業者に対して，テロや内通者を含む脅威[g] を想定した非常に厳格で具体的な規制を行っており，その規

e）：NERC（North American Electric Reliability Corporation：北米電力信頼性評議）
北米各地の電力の安定供給を目的に，電力業界や連邦政府，州政府などにより 1968 年に創設された。

f）：米国の原子力規制委員会（NRC: Nuclear Regulation Commission）
非軍事目的で使用される，放射性物質の安全使用を確保する機関であり，1974 年に設立された。米国内の原子力施設は，NRC の規制に従わなければならない。

図―５　さまざまなログやイベントを収集して状況認識を実現する SIEM

制を守るための対策を示したガイドラインを提供している[h)]。

そのガイドラインの基本戦略は「多層防御」だ。簡単にいうと，セキュリティ対策を多重に施すことで，たとえ内通者がいたり，テロに遭ったとしても，どこかで食い止めようという考え方である。アンチウイルス等のウイルス対策を行うのはもちろんだが，それだけでは破られてしまうかもしれないので，ネットワークに流れるデータに不正なものがないか監視したり，放射能漏れなど重大事故を引き起こす可能性のある設備に対しては，外からは一切操作できないようにして，モニタリングだけ可能にするといった考え方だ。特に，重大事故につながる恐れのある設備は，権限のある人でも外からは操作できない。ここでは，データの流れを一方向に制限するデータダイオードと呼ばれる製品が用いられていることが多い。この製品はハードウェアで逆方向の通信を遮断する仕組みをとっていて，脆弱性をもつ可能性があるソフトウェアで遮断を行う場合よりも強固な仕組みを提供している。

もうひとつの重要な考え方として，「状況認識」があげられる。ここでいう「状況認識」とは，システム全体のログやイベント情報を集めて相関分析を行い，早期に異常を察知し対策を行うことである。これは，特に産業インフラを支える制御システムに対しては大事な考え方である。先にも述べたように，制御システムは可用性を重視するため古いシステムが残り続けることが多く，攻撃を受けやすい環境にある。したがって，さまざまなソリューションで防護することも重要だが，ある程度攻撃が成功してしまう前提で，いかに早く攻撃に気づいて対策が打てるかがポイントであり，そのため「状況認識」の実現が重要だと言われている。状況認識を実現するツールとしては，SIEM（System Information and Event Management）というソリューションが知られている（**図―５**参照）。

6. 日本における課題と望まれる姿

ここまで，世界における産業インフラに対するサイバー攻撃とセキュリティ対策の実情を見てきたが，それを踏まえて，日本における課題と望むべき姿について概観して締めくくりとしたい。

今後，東京オリンピック・パラリンピックを控えて，日本が世界的な注目を集めるなかで，産業インフラをサイバー攻撃からどのように守るかということは，これまで以上に重要な課題となっている。

しかし，日本における最大の課題は，仮に産業インフラ事業者が脅威を理解したとして，何をどこまで対策しなければならないのかの拠り所がない点である。セキュリティ対策がコストとしか見なされない現状では，このままでは何も対策が進まないだろう。電力業界においては，既にガイドラインの策定が進められて

g)：設計基礎脅威（DBT：Design Basis Threat）と呼ばれる。核物質防護システムを設計する上で考えなければならない脅威のことで，サイバーに限らず，テロや内通者を想定した原子力施設の設計基礎となる脅威。

h)：米国の NRC が定めるサイバーセキュリティの基準は以下の２つのドキュメントに示されている。
「Title 10 Code of Federal Regulations（CFR），section 73.54（10 CFR 73.54)」
「Regulatory Guide 5.71（RG5.71)」
10 CFR 73.54 では，全ての原子力施設において，安全，セキュリティ，緊急対策に関係するコンピュータ，通信システム，ネットワークを保護することが規定されており，RG5.71 はこのレベルのセキュリティを実現するための具体的な手順を提供している。

いるが，他の産業インフラ業界でも同様の取り組みが求められると考える。

世界で産業インフラへのサイバー脅威へのセキュリティ対策が進む中で，日本も官民一体となって問題に取り組み，産業インフラ事業者がどのようなセキュリティ対策を取れば良いのかが示されている状態を目指して進むべきではないか。

JCMA

［筆者紹介］
佐々木　弘志（ささき　ひろし）
インテル セキュリティ（マカフィー㈱）
サイバー戦略室
CISSP