SE Report

重要インフラ事業者が理解するべきサイバーセキュリティの動向

セコム株式会社 IS 研究所
コミュニケーションプラットフォームディビジョン　マネージャー
松本　泰 Yasushi Matsumoto

1. はじめに

重要インフラへのサイバー攻撃により、重大な被害が引き起こされる可能性が現実のものとなりつつあります。現在、サイバー攻撃に関する記事などを毎日のように目にしますが、これまでのところ、サイバー攻撃による被害の多くは「なりすまし」による金銭被害や、個人情報が大量に盗み取られるといった事例が挙げられます。例えば、2015年の日本年金機構におけるサイバー攻撃（不正アクセス）では、約125万件にも及ぶ個人情報の流出があったとされています。

このサイバー攻撃の対象は、時代と共に変化拡大していることに注意する必要があります。そして、今後の考えられるサイバー攻撃の対象となりつつあるものに、重要インフラないし重要インフラを制御する制御システムがあります。

この重要インフラへのサイバー攻撃において最も懸念されていることは、重要インフラの制御システムを機能不全にさせることにより、重要インフラが提供している社会生活にとって必要不可欠なサービスを、停止ないし低下させるといったものになります。

こうしたこともあり、重要インフラのサイバーセキュリティに関するさまざまな活動が始まってはいます。しかし、多くの重要インフラ事業者は、さほど事例も多くない重要インフラへのサイバー攻撃に懐疑的かもしれません。また、サイバー攻撃に関する認識があったとしても、手品のようにも見えるサイバー攻撃の話に対して、どのように対処するべきなのか戸惑っているのが現状ではないでしょうか。

本稿では、重要インフラ事業者などが認識するべき重要インフラへのサイバー攻撃が可能になっている背景と、その対応の方向性について説明します。

2. サイバーセキュリティに関する歴史

本稿のテーマである「重要インフラのサイバーセキュリティ」を説明する前に、重要インフラがサイバー攻撃の対象になりつつある現在までのサイバー攻撃と、サイバーセキュリティに関する歴史的な概観について説明します。

サイバーセキュリティの類似語に「コンピュータセキュリティ」、「ネットワークセキュリティ」、「情報セキュリティ」などがあります。この中で、歴史的に最初によく使われた用語は「コンピュータセキュリティ」になります。これは、インターネット普及以前の80年代から90年代前半のネットワークがまだ発達していなかった時代によく使われた用語になります。

その後、インターネットの普及と共にインターネット越しの攻撃に対応するための

「ネットワークセキュリティ」が浮上しました。90年代後半においてインターネット越しの攻撃は、主にインターネットに直接接続されたインターネットサーバへの攻撃を意味しました。

2000年代になると「情報セキュリティ」という用語が浮上してきました。情報セキュリティは、守るべき対象を「情報資産」として、この「情報資産」をいかに守るのかと言った考えに基づいた用語になります。「情報セキュリティ」が浮上した背景には、インターネットが普及し情報通信技術が急速に発展する中、非常に重要な情報（すなわち情報資産）をコンピュータ上に置き、また、こうした情報を外部とやりとりすることがごく当たり前になってきた時代背景があります。

2000年代後半になると、インターネットに直接接続されたサーバだけではなく、オフィスネットワークの中の「情報資産」も攻撃の対象となるようになり、標的型攻撃（Advanced Persistent Threat：APT）攻撃と呼ばれる攻撃技術の高度化も進んできました。2015年の日本年金機構へのサイバー攻撃もこうした標的型攻撃の事例の一つと言えます。

2016年現在、「サイバーセキュリティ」という用語がより多く使われるようになってきました。例えば、2014年11月には「サイバーセキュリティ基本法」が成立・施行され同時に「内閣官房情報セキュリティセンター」は「内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity：NISC）」に改編されています。

「サイバーセキュリティ」という言葉がより多く使われるようになってきた背景の一つは、サイバー攻撃の対象が従来からの情報資産などを格納し処理する情報システムだけではなく、従来は安全だと思われていた重要インフラなどを制御する制御システムにも向かっており、守るべき対象が変化拡大してきたことがあります。

以上のように、サイバー攻撃の対象は時代と共に変化拡大しており、今後は重要インフラなどを制御する制御システムがサイバー攻撃の対象となりつつあるということを、まずは理解する必要があります。

3. 制御システムへの攻撃が可能になってきた背景

従来、重要インフラにおける制御システムは、インターネットなどから隔離されたクローズドネットワークで構成され、また、一般の情報システムと異なり、多くの独自技術、独自システムで構成されているために安全だとされてきました。

現在、こうした安全神話を覆すサイバー攻撃の事例が出てきています。重要インフラ事業者などは、この重要インフラの制御システムなどへのサイバー攻撃が可能になってきた背景を十分に理解する必要があります。

重要インフラの制御システムなどへのサイバー攻撃が可能になってきた背景には、大きく以下の3つが考えられます。

（1）重要インフラにおける制御システムの標準化、汎用化、コモディティ化
（2）重要インフラの制御システムにおけるさまざまな情報連携の要求
（3）制御システムへの攻撃手法の拡散

（1）に関して、従来、重要インフラなどの制御システムは、独自技術の組み合わせで構築されることが多かったと言えます。しかし現在は、情報通信技術が急速に発達する中、標準化などが進み、高い相互運用性を持ったソリューションで構成されることが多くなっています。制御システムは独自から汎用化、コモディティ化（無差別化）の道を進んでお

り、また、基本ソフトであるLinuxなどの多くのオープンソース※1も使われるようになってきています。こうしたことは、攻撃者が、攻撃対象としての（制御）システムの構成などを容易に類推することが可能になってきたことを意味します。

次に（2）に関して、重要インフラにおいて、その中核を担う制御システムと他のさまざまなシステムとの情報連携の要求が増えてきたということがあります。そもそも重要インフラにおける制御システムは、元はと言えば、スタンドアローンな制御機器が、運用・保守などの観点や、制御機器同士の連携の要求などからボトムアップにネットワーク（クローズドネットワーク）に接続されてきたという歴史があります。現在では、こうしたクローズドネットワークが、更なる効率性、保守性、利便性などの要求から「なし崩し的なオープンネットワーク化」に向かっている場合があります。例えば、ビルにおける空調制御システムは、省エネや快適性などを実現するため、他の情報システムとの連携を要求されつつあります。このビルにおける省エネなどは、社会の要請でもあることに注意する必要があります。スマートビル、スマートシティ、スマートグリッドといったスマートな社会（賢い社会システム）を目指した事例の多くは、重要インフラの制御システムと他の情報システムとの連携によりその実現を目指しています。

重要インフラ事業者がサイバーセキュリティを強化すべき理由は、社会の要請として、また業種によってはサービスの競争力強化のために情報連携が必要になっており、その情報連携を進めるためにはサイバーセキュリティの強化が必要になっていると考えるべきでしょう。

（3）に関して近年、重要インフラの制御システムへのサイバー攻撃の（成功）事例が報告されています。こうしたこともあり、制御システムへの攻撃の手法自体も広く知られてきたということがあります。これまで重要インフラの制御システムは、「攻撃が出来ないと思われていたために」サイバー攻撃の対象となっていなかった側面が多々あります。しかし、サイバー攻撃の成功事例が報告され、攻撃が出来ると認識された故に、重要インフラがサイバー攻撃の対象になりつつあるというのが現在の状況と言えます。

ここで説明した3つの背景の中で、(1), (2)は、重要事業者自身の問題ですが、これらは徐々に進行してきているため、多くの重要事業者などが、気が付いていない場合も多いと考えられます。こうした状況に加え（3）の状況が大きく変化しており、こうしたことにより重要インフラの制御システムへの攻撃が可能になってきたということを十分に認識する必要があります。

4. イラン核協議「歴史的合意」とサイバー攻撃

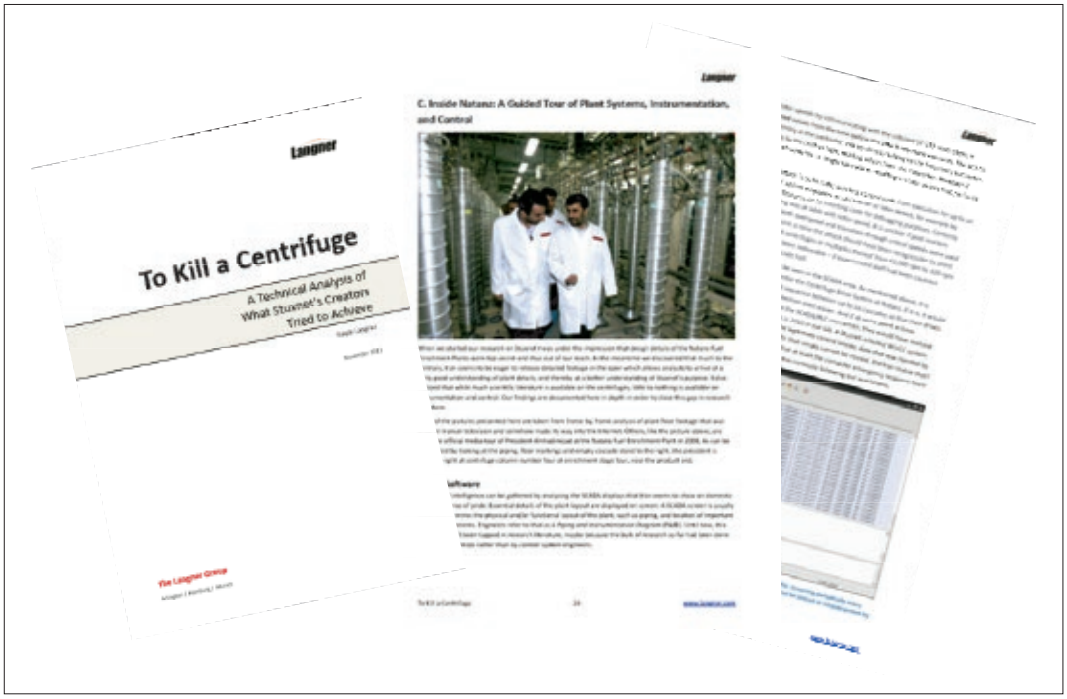
それでは、いつ頃から重要インフラの制御システムへのサイバー攻撃が可能ということが世の中で認識されるようになったのでしょうか。攻撃が可能と認識される一つのきっかけに「スタックスネット[1)]」と呼ばれるコンピュータワームによるサイバー攻撃があります（**図1**）。

この「スタックスネット」によるサイバー攻撃は、2015年7月の「イラン核協議の歴史的合意」と、この合意に基づく2016年1月の「イラン制裁解除」に関係があります。この「イラン核協議の歴史的合意」における最重要合意事項の一つに、イラン中部のナタンズにある核濃縮施設のウラン濃縮に使う遠心分離機の数を1/3以下に減らすというものがありました。

この「ナタンズ核濃縮施設のウラン濃縮に

※1
オープンソース
（open source）無償で公開されているソフトウェアを作るためのソースコード。だれでもその改良や配布ができるようになっている。

図1　スタックスネット[1)]



使う遠心分離機」は、「イラン核協議の歴史的合意」以前の2010年に「スタックスネット」によるサイバー攻撃を受けたことが発覚しました。こうしたことにより、ウラン濃縮に使う遠心分離機のような制御システムへのサイバー攻撃が可能なことを、世に知らしめる結果となりました。

この遠心分離機へのサイバー攻撃に関して、サイバー攻撃を受けたイランからは報告されていないこともあり、実際にどのような手順でサイバー攻撃が行われたかは必ずしも明らかではありません。しかし「スタックスネット」自体のプログラムの解析などの結果からさまざまな「スタックスネット」に関する報告書などが発行されています。こうした報告書により「スタックスネット」によるサイバー攻撃の実態が明らかになった一方、攻撃者視点からも、制御システムへの攻撃が可能な事や攻撃手法自体も広く知られることになりました。

「スタックスネット」による攻撃は、核濃縮施設を完全に停止されるというものではなく、遠心分離器を微妙にコントロールし核開発の現場を混乱させるというものでした。サイバー攻撃は2008年頃から行われていたと推測されていますが、つまり2年間もその存在自体が隠され続けた訳です。そして2010年に「スタックスネット」の存在が発覚した直後には、遠心分離機への一斉攻撃がなされています。

この「ナタンズ核濃縮施設のウラン濃縮に使う遠心分離機」の制御システムは、PLC（Programmable Logic Controller）とそのPLCに命令を出すWindowsのパソコンの制御プログラムなどから構成されていたのですが、このWindowsのパソコンの制御プログラムが「スタックスネット」により改ざんされ遠心分離機の制御が攻撃されました。この制御に使われたPLCは、多くの重要インフラの制御システムでも使われている製品だったのですが、これは、さまざまな重要インフラの制御システムが攻撃可能なことを示唆することになったと言えます。

2016年のイラン経済制裁解除に至った合意により、核拡散は防がれる方向に向かいましたが、核拡散を防ぐことを一つの目的とし

た「制御システムへのサイバー攻撃」は、「スタックスネット」以後、世界中に拡散して行く結果になったと言えます。

5. 重要インフラにおける対策の取り組み

ここまで、重要インフラの制御システムへの攻撃が可能になってきた背景と、重要インフラの制御システムへの攻撃が可能ということが世の中で認識されるきっかけとなった「スタックスネット」の事例を説明しました。では、こうした現状に対して重要インフラ事業者などは、どういった対応を行うべきなのでしょうか。

現在、重要インフラの制御システムに関するさまざまな取り組みがあり、例えば2012年には、技術研究組合・制御システムセキュリティセンター[2)]が設立されるなど、重要インフラの制御システムのセキュリティ確保に関するさまざまな活動が活発化しています。しかし、重要インフラの制御システムと言ってもさまざまであり、その対策は、重要インフラ事業者自らが取り組む必要がありますが、まずは、実態を把握するとともに、次の二つの観点を見て行く必要があります。

(1) 制御システムのクローズドネットワークの見直し
(2) 制御システムのネットワークに接続された制御機器の対策

おおむね、(1) は、中短期的な取り組みとして重要になり、(2) に関しては、短期的な取り組みでは解決せず、システム刷新時などの取り組みなど中長期的な取り組みも必要になるでしょう。

「(1) 制御システムのクローズドネットワークの見直し」に関しては、まずは、隔離されたネットワーク（クローズドネットワーク）の実態を把握することが重要になります。それには、3つの点に注目する必要があります。

一つ目に、クローズドネットワーク自体は、まずは、物理セキュリティで十分に守られている必要があります。

二つ目は、クローズドネットワークに侵入する可能性としてネットワーク経由だけとは限らないということがあります。近年の事例では、USB メモリによりクローズドネットワークに接続された機器にコンピュータウィルスが感染した事例が多数報告されています。また「スタックスネット」も USB メモリ経由で侵入されたと推測されています。

三つ目は、クローズドネットワークと言いつつ、何らかの理由で他のネットワークと接続されている場合があり、その実体を正確に把握することです。例えば、インターネットには直接接続されていないけれどオフィスネットワークとつながっている。また、制御機器のリモートメンテナンスのため保守ベンダーとつながっているといった事例があります。2013年、米国の小売大手事業者である Target 社から4,000万件のクレジットカード情報が漏洩[3)]しましたが、この情報漏洩は、Target 社の空調をメンテナンスする事業者のリモートメンテナンス回線がなりすまされたのが、その攻撃のきっかけになっています。

制御システムのクローズドネットワークにとってオフィスネットワークもリモートメンテナンスを行う保守ベンダーも信頼のおける接続先のはずだったのかもしれませんが、現在は、こうした信頼のおけるはずの接続先自体が、サイバー攻撃の対象となっていることを忘れてはなりません。

以上のようなことに対する対応、対策の基本は、クローズドネットワーク自体のボーダーとなる物理セキュリティの見直しや、運用要員の教育と言った地道な見直しが非常に重要になります。

「(2) 制御システムのネットワークに接続された制御機器の対策」に関して、元々、多くの制御システムのネットワークに接続された制御機器は、隔離されたネットワーク（クローズドネットワーク）を前提に作られてきたこともあり、ネットワークセキュリティ的には、脆弱性を内在している制御機器が多いのが現実です。

またクローズドネットワークを前提で作られてきた制御機器は、インターネット上では当たり前になっている暗号技術を利用した認証や暗号化が実装されてないことが多いと言えます。制御機器などに暗号技術を組み込んだ経験がない制御機器ベンダーにとっては、こうした暗号技術を使いこなすことは容易ではなく、今後の大きな課題となるでしょう。

個々の機器における脆弱性や暗号技術の組み込みは、その対策コストも含め非常に時間がかかることが予想されます。従って「(1) 制御システムのクローズドネットワークの見直し」が非常に重要になる訳ですが、最終的には個々の機器における脆弱性対策なしに、今後の社会の要請とも言える重要インフラと他システムとのさまざまな情報連携を進めることは難しいということを十分に認識する必要があります。

以上は、重要インフラにおけるサイバーセキュリティの対策のある側面に過ぎず、より多角的な観点からのサイバーセキュリティの対策が必要になると考えられます。

6. おわりに

本稿では、過去から現在までのサイバーセキュリティの動向を概観することにより、重要インフラ、重要施設でのサイバーセキュリティに取り組む重要性を説明しました。

一般的に重要インフラ、重要施設の設備は、一般の情報システムより長いライフサイクルを持ち、サイバーセキュリティの対応を根本的に行うには、非常に時間がかかると考えられます。非常に時間がかかるからこそ、既存の重要インフラのサイバーセキュリティの対応は、喫緊の課題と認識するべきでしょう。

また、重要インフラにおける設備システムの新規の構築や、刷新時などにおいては、後付けのサイバーセキュリティの対策だけではなく、設計時における、サイバーセキュリティを考慮した設計（セキュリティ・バイ・デザイン）が望まれます。

今後の社会において、社会基盤である重要インフラと他のシステムの情報連携などへの要求は強まっていくことは間違いなく、また、情報連携も含めてサイバーセキュリティ対応は必須要件になっていくことは間違いありません。本稿がそうした対応に多少でも参考になるようであれば幸いです。

参考文献

1) To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve, Ralph Langner, 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
2) 技術研究組合・制御システムセキュリティセンター http://www.css-center.or.jp/index.html
3) "A 'Kill Chain' Analysis of the 2013 Target Data Breach" report11, for the Senate Committee on Commerce, Science, and Transportation, issued on March 2014, http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf

まつもと●やすし

セコム株式会社 IS（Intelligent Systems）研究所勤務。計測分野、情通通信分野、情報セキュリティ分野の企画、研究、設計、開発、運用に従事。2007年経済産業省商務情報政策局長表彰「情報セキュリティ促進部門」受賞。2012年12月より現職。