制御システムセキュリティの重要性と現状

第2回 原子力分野における制御システムセキュリティ

技術研究組合 制御システムセキュリティセンター

(株)三菱総合研究所

村瀬 一郎

近年、制御システムセキュリティが話題となっている。特に、原子力分野においては、2010年にイランの核燃料施設に対して STUXNET と呼ばれるマルウェア (攻撃プログラム) によりサイバー攻撃が行われ、サイバーセキュリティ対策の必要性の認識が浸透しつつある。本稿では、原子力分野における制御システムセキュリティの脅威動向と対策の方向性、国際機関等における対応動向を述べる。

I. はじめに

以前より、IT 分野のサイバーセキュリティ対策は、インターネットに接続されるシステムや、金融系のシステム等 (これらを情報システムと呼ぶ) において問題となってきた。しかし、世の中には、情報システム以外に、制御システムが存在する。制御システムは、プラントや工場、ビルにおいて、タービン、ボイラ、空調、照明等の機器を制御する役割を担っている。こうした制御システムに対するサイバーセキュリティ上の脅威は、2010 年 10 月にイランの核燃料施設に対する STUXNET と呼ばれるマルウェア (攻撃プログラム) によるサイバー攻撃が報告され、制御システムの関係者の間で脅威が広く認識されるようになった。また、STUXNET により遠心分離機が物理的に破壊されたことが報告され、原子力分野の制御システムにおけるセキュリティ対策の必要性が叫ばれるようになった。

II. STUXNET^{1~4)}

STUXNET は、2010 年 7 月中旬に出現し、Windows や Siemens のソフトウェアの脆弱性を悪用し、結果的に遠心分離機の破壊に至った。攻撃対象は、イランのナタンズの核燃料物質関連施設であり、クローズドなシステムに侵入し、遠心分離機に物理的な損害をもたらすに至った。これによって、制御システムはクローズであるため安全であるという関係者の認識は大きく変貌した。

Significance and Status of Control System Security (2) ; About the industrial control systems security in the nuclear sector : Ichiro MURASE.

(2014 年 3 月 24 日 受理)

STUXNET の動作概要を次に示す。

- (1) STUXNET が制御システムまたは近傍の情報システムに侵入：USB メモリー等可搬型デバイス、または情報システムからの侵入 (Windows のネットワーク関係サービスの脆弱性を悪用した可能性が指摘されている) により STUXNET が制御システムへ侵入する。
- (2) Windows パソコンにおける管理者権限の取得：STUXNET は、Windows パソコンの脆弱性 (実際の攻撃時点では未知の脆弱性であり、未知の脆弱性を利用した攻撃をゼロデイ攻撃という) を悪用し、管理者権限を取得する。
- (3) 制御システム内で特定のソフトウェアが稼働するエンジニアリング端末に侵入
- (4) STUXNET は、Windows システムフォルダを検索することにより、Siemens の SIMATIC WinCC あるいは SIMATIC PCS 7 (いずれも Siemens が提供する制御システム向けの監視制御システムであり、端末側にはエンジニアリング機能を有する) 端末が稼働する Windows パソコンを探し当てる。
- (5) 攻撃コードのダウンロード：STUXNET は、SIMATIC WinCC または SIMATIC PCS 7 が稼働するパソコン上で、Siemens のコントローラ (PLC) のコードを攻撃コードに変更する。概要は、次の通り。
 - ・CPU が 6ES7-417 および 6ES7-315-2 である PLC を攻撃対象とする。
 - ・当該 PLC は、周波数変換装置を制御しており、STUXNET は、807 ~ 1,210Hz の高周波数部分の制御を攻撃対象とする。

- ・何か月にもわたって、周波数変換装置の出力周波数を短時間のうちに 1,410Hz, 2Hz, 1,064Hz と順に変化させる。

この結果、遠心分離機が過負荷となり、全体の 10% が物理的損害を被ったと言われている。

なお、上記の(1)～(5)以外にも STUXNET は様々な特徴を有している。代表的な特徴を次に示す。

- (a) STUXNET は、ファイル共有機能の脆弱性を利用して自らを他のパソコンにコピーし増殖
- (b) ルートキットと呼ばれる機能を有し、操作者が STUXNET の存在を認知することを阻止
- (c) 監視制御システム (SCADA) を乗っ取り、ディスプレイ上に異常状態であることを表示せず、通常状態であることを表示
- (d) イランのナタンズの核燃料施設のシステムを標的とした攻撃

このように、STUXNET は非常に高度な機能を有するサイバー兵器であり³⁾、多額のコストをかけて作成されたことが推察される。

Ⅲ. STUXNET への対策

STUXNET への対策を検討する上で重要な視点は次の通りである。

- (a) 複数の公表されていない脆弱性を悪用していること
- (b) USB メモリーが初期感染源である可能性があること
- (c) ディスプレイにおける表示データと実際のデータが異なっていたこと
- (d) 標的となった核燃料施設を十分に調べたサイバー攻撃であること
- (e) クローズなシステムに対して攻撃がなされたこと

上記の視点に沿って、対策を述べる。

- (a) 複数の公表されていない脆弱性を悪用している (ゼロデイ攻撃である) こと

制御システムにおいては、端末やサーバにセキュリティパッチを適用することは、可用性重視の観点から難しい場合が多い。さらにはゼロデイ攻撃の場合、セキュリティパッチ自体が配布されていないためセキュリティパッチを適用することは不可能であり、セキュリティパッチ適用による対策をすることはできない。セキュリティパッチ適用が困難な場合の対策として、ホワイトリスト技術が注目を集めている⁴⁾。ホワイトリストとは、サーバや端末においてはあらかじめ決めたソフトウェアの動作 (ホワイトリスト) に従ってソフトウェアの動きを制限し、通信機器においてはあらかじめ決まった通信 (ホワイトリスト) のみを許可する技術である。ホワイト

リストは、制御システムで重要であるリアルタイム性確保の点からも有望とされている。

- (b) USB メモリーが初期感染源である可能性があること

STUXNET は USB メモリーを介してシステムに侵入した可能性が指摘されている。USB メモリーによるマルウェア感染を防止するためには、USB メモリーを利用不可能とすることが必要である。それには、USB ポートを塞ぐまたは着脱する、USB ポートへの I/O バスを外す、USB ポート管理エージェントを導入し USB ポート利用の際には上司の承認を必要とする等の対策がある。また、USB メモリーをやむを得ず利用する場合、USB メモリー装着前にスタンドアロンパソコン (ネットワークから切り離されたパソコン) でウイルスチェックすることは必須である。

- (c) ディスプレイにおける表示データと実際のデータが異なっていたこと

表示データと実際のデータが異なっていた理由は、SCADA の未知の脆弱性を悪用したことによる。現場においては、表示系が常に正しいわけではないことを念頭に置き、実際のデータを現場から収集するシステムを SCADA とは別に実装する (デジタルではなくアナログで実装する方式も考えられる)。

- (d) 標的となった核燃料施設を十分に調べたサイバー攻撃であること

STUXNET のようなサイバー兵器の製造のためには、サイバー空間のみならずリアル空間での事前の綿密な調査が行われていることが推察される。このような綿密な調査が行われるか否かは、攻撃側と防御側を取り巻く安保情勢に依存する。STUXNET は、イランとその周辺国および欧米諸国との不安定な関係が背景にあったと考えられる。防御側がこうした安保情勢を認識することが対策の第一歩となる。

- (e) クローズなシステムに対して攻撃がなされたこと
クローズなシステムにおける脅威と対策はⅣ章にて述べる。

Ⅳ. 我が国原子力分野における制御システムの現実的な脅威と対策

STUXNET は事前に標的を綿密に調査した標的型攻撃であり、我が国の原子力分野において、この種の標的型攻撃が現実的な脅威となりうるかは不明である。そこで、本稿では我が国原子力分野における制御システムの現実的な脅威と対策について述べる。

原子力分野に限らず、制御システムは一般的にクローズであると考えられている。こうしたクローズであると考えられているシステムの脅威と対策は、次に示すこと

ができる⁵⁾。

(1) USB ポートの利用

USB ポート利用への対策はⅢ章に挙げた通りである。

(2) リモート監視システムによる外部ネットワーク接続

コントローラの制御対象機器は、高価な機器であることも少なくない。こうした高価な機器の場合、問題発生時への対応のためにベンダがリモート監視回線を設置することがある。リモート監視回線に係る脅威は、通信経路で盗聴される可能性があること、不適正な端末をリモート監視端末として接続される可能性があること等がある。

こうした脅威への対策は、リモート監視システムを専用線により構築し暗号化通信を行うこと、リモート監視端末にはクライアント証明書をダウンロードし認められた端末以外はリモート監視端末として利用できないことにする、リモート監視端末におけるセキュリティ検査を実施する等がある。

(3) 操作端末の入れ替え

日本のある自動車会社では、2009年にエンジニアリング端末入れ替え時に、ベンダが持ち込んだエンジニアリング端末にコンピュータウイルスが混入し、組立ラインの応答が3日間程度低下した。

こうした脅威を防止するためには、ベンダが持ち込んだPCの場合でも、ネットワークに接続する前にウイルスチェックを行うことが必要である。

(4) 物理セキュリティの突破

物理セキュリティを突破された場合、サイバーセキュリティ上最も重要な脅威は、通信機器の空きポートに通信ケーブルが接続され、正規ではないパソコンによるエンジニアリング端末や監視制御端末に成りすましが実行される可能性があることである。また、USBポートは様々な機器に装着されており、USBポートからマルウェアを感染させることも可能である。

こうした脅威への対策は、入退室管理の徹底(立ち入りに係る事前申請の徹底、二要素認証、持ち物検査、共連れ防止、体重検査、ドア鍵管理等)、通信機器における物理対策(通信機器の物理的管理の徹底等)等が挙げられる。

V. 国外におけるサイバーセキュリティ対策の動向

原子力規制庁は、NRCとIAEAの動きを次のように述べている。⁶⁾

「NRC(米国原子力規制委員会)は2001年から本格的に取り組む始め、2009年に全原子炉に対しサイバーセキュリティに関する義務化を行い、さらに2010年にはガイドラインを発表している。IAEAも2011年に核施設におけるコンピュータセキュリティに関するガイドラ

インを発表し、メンバー諸国にも積極的に対策と訓練を行うように促している。日本国内の原子力発電所におけるサイバーセキュリティも世界と同レベルで万全の対策を取っていくことが必要である。」

2013年7月1日国際原子力機関(IAEA: International Atomic Energy Agency)は、核セキュリティ国際会議を開催し、核セキュリティに関する国際会議(グローバルな努力の強化)閣僚宣言を採択した^{7, 8)}。サイバーセキュリティに関しては、次のように述べられている。

「サイバー攻撃に対する認識を高めるIAEAの努力を認識し、IAEAがこの分野での国際協力を促進して、国家を支援する更なる努力を行うことを奨励。」

さらに、IAEAはサイバーセキュリティに関して様々な取り組みを行っており、その概要を述べる^{7, 8)}。

IAEAは、制御システムへのサイバー攻撃が新たなトレンドになりつつあると述べ、制御システムにおける脅威は次を挙げている。

- ・リモート監視
- ・USBメモリー等可搬型デバイス
- ・サプライチェーン
- ・物理攻撃を伴う攻撃
- ・SNS(Social Networking Service: インターネット上の会員向け情報交流サイト)を用いた情報収集や個人への接近
- ・無線通信
- ・ゼロデイ攻撃

また、IAEAはサイバーセキュリティ対策として次の活動を行っている。

- ・ガイドラインの作成
- ・情報交換会(フォーラム)の開催
- ・地域での訓練の開催
- ・地域や世界的な演習の開催
- ・インシデントレスポンス(緊急時対応)習熟のための情報提供
- ・その他の普及啓発活動

VI. まとめ

原子力分野のサイバーセキュリティ対策は決して海外のみの問題ではなく、我が国においても差し迫った問題である。IAEA等国際機関や標準の動向を念頭に置きつつ、我が国における原子力分野の制御システムのサイバーセキュリティ上の脅威を客観的に分析し対策することが重要である。

ー 参考資料 ー

- 1) 日本シーサート協議会: マルウェア STUXNET(スタクスネット)について,
<http://www.nca.gr.jp/2010/STUXNET/>, 2010.10
- 2) トレンドマイクロ: 「STUXNET」ファミリがSCADAシステ

- ムを狙う！、
<http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=STUXNET+Malware+Targets+SCADA+Systems>, 2010.10
- 3) ニューズウィーク日本語版：産業サイバー兵器スタックスネットの防ぎ方,
<http://www.newsweekjapan.jp/stories/world/2010/10/post-1683.php>, 2010.10
- 4) 猪股晃匡：STUXNET の脅威と今後のサイバー戦の様相,
<http://www.bsk-z.or.jp/kenkyucenter/pdf/23kennshouronnbunnjyushousakuhinn.pdf>, 2012
- 5) 技術研究組合制御システムセキュリティセンター：CSSC のご紹介,
http://www.css-center.or.jp/pdf/about_CSSC_ppt.pdf, 2013/12
- 6) 原子力規制庁：福島第一原子力発電所事故を踏まえた国内外での教訓,
https://www.nsr.go.jp/committee/yuushikisya/shin_anzenkijyun/data/0001_09.pdf

- 7) 外務省：IAEA 核セキュリティ国際会議(概要)
http://www.mofa.go.jp/mofaj/gaiko/page3_000286.html, 2013/07
- 8) IAEA：核セキュリティに関する国際会議：グローバルな努力の強化 閣僚宣言(骨子)
<http://www.mofa.go.jp/mofaj/files/000007118.pdf>, 2013/07
- 9) 国際原子力機関：Office Of Nuclear Security Cyber Security Programme,
http://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf, 2013.05

著者紹介

村瀬一郎（むらせ・いちろう）

（株）三菱総合研究所

制御システムセキュリティセンター

（専門分野/関心分野）制御システムセキュリティ/情報セキュリティ

学会誌への投稿記事の採否に関する判断基準

日本原子力学会 編集委員会

学会誌への投稿は、記事原稿の作成に先立ち、記事提案書(学会 HP に記載)の提出が必要となります。提出された記事提案書は編集委員会で審議し、通過したものについて記事原稿を提出していただくことにしています。

投稿記事の内容については著者に責任がありますが、記事提案書の審議において、投稿記事が下記のいずれかに該当すると判断した場合は、学会誌に掲載することをお断りすることになっています。なお、記事提案書に基づいて執筆された記事原稿につきましても、下記のいずれかに該当すると判断した場合や、記事提案書と異なる内容の原稿が提出された場合は、掲載することをお断りすることになっています。

- (1) 事実を無視し、あるいは歪曲した意見。
- (2) 真偽が不明な内容を含む場合。
- (3) 文章に論理性がない場合。文章が意味不明な場合。
- (4) 掲載することにより、学会の品位に傷がつく恐れがある場合。
- (5) 良識に欠けると思われる意見。例えば、個人あるいは組織の中傷・誹謗、一方的な極め付けなど。
- (6) 美醜、好悪に類する判断に依拠している場合。
- (7) すでに掲載された記事と同様の内容である場合。
- (8) 商業的な広告・宣伝などを目的とする場合。
- (9) 会員にとって掲載する価値がない場合。
- (10) 余り期間を空けない同一者からの投稿。

(註1) 記事提案書の審議結果については約1か月で事務局よりお知らせいたします。

(註2) 掲載否の場合、該当事由の番号をお知らせしますが、それ以上の説明は致しません。

(改定 2012 年 6 月 1 日)