サイバー戦入門　その６

－制御システムへのサイバー攻撃とその対策－

三村　守（防大情報工学科）

１　はじめに

制御システムは、製造業をはじめとした産業領域で利用されている他にも、電力、水道、ガス等、鉄道の国民生活の基盤となるサービスを提供するために利用されている。かつて、制御システムは独自の仕組みで動作しており、分離された独立したシステムであることがほとんどであった。そのため、サイバー攻撃やマルウェアとは無縁という安全神話があり、積極的にセキュリティ対策が講じられることはなかった。しかしながら、コンピュータやインターネット技術の普及に伴い、利用者の利便性が向上するとともに、制御システムもこれらと共通の仕組みで動作するようになってきた。これは、これまでインターネットやこれに接続するＬＡＮ[1]を中心に構成されていたサイバースペースが、制御システムのネットワークにも拡大したことを意味している。そのため、制御システムにおいても、サイバー攻撃やマルウェアによる物理的な被害が発生するようになってきた。例えば、石油のパイプラインが爆発した事例では、制御システムがサイバー攻撃を受けた可能性が指摘されている。また、電力会社がサイバー攻撃を受け、大規模な停電が発生した事例もある。とりわけ、２０１０年６月に発見されたＳｔｕｘｎｅｔ（スタックスネット）と呼ばれるマルウェアには、核燃料施設の産業用制御システムを攻撃する機能が含まれていたことから世界に衝撃が走った。このように、今や制御システムの安全神話は完全に崩壊しており、より一層高いセキュリティ対策が求められるようになってきている。

一般に、サイバー攻撃やマルウェアは、論理的な仮想世界であるサイバースペースにおいてサービスの停止や情報漏洩等の被害をもたらすものであり、物理的な現実世界において直接的な被害をもたらすことはないと考えられてきた。しかしながら、制御システムでは、コントローラの制御が奪われることにより、物理的な現実世界においても被害を発生させる危険性を秘めている。この物理ドメインに干渉するという特性は、仮想世界と現実世界を結び付けるものであり、極めて重要である。また、制御システムは、国民生活および社会活動に不可欠な重要インフラ[2]を構成する要素でもある。したがって、制御システムに対するサイバー攻撃は、国家の安全保障や軍事作戦を考える上でも極めて重要な要素である。

「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」では、サイバー攻撃とは何かを理解するために必要な基本的な仕組みを、技術的な観点から体系的に解説することを試み、「サイバー戦入門　その２　－サイバー戦の概念と作

---

[1]LAN（Local Area Network）

[2]電力、水道、ガス等の国民生活および社会活動に不可欠なサービスを提供する社会基盤のこと

戦－」ではサイバー戦の概念とサイバー作戦の種類について平易に解説することを試みた。その３からは、サイバー戦に関する各トピックスをより掘り下げて平易に解説することを試みている。本稿では、制御システムへのサイバー攻撃とその対策をとりあげる。以下、第２節では制御システムへのサイバー攻撃の具体例を挙げ、第３節では制御システムの概要について説明する。第４節では制御システムへのサイバー攻撃の仕組みについて説明する。第５節では、サイバー攻撃への対策について説明し、最後にまとめと課題について述べる。

２　制御システムへのサイバー攻撃の具体例

（１）初期の制御システムへのサイバー攻撃

公表されている最初の制御システムへのサイバー攻撃の事例は、２０００年２月から４月にかけて、オーストラリアのＭａｒｏｏｃｈｙ　Ｓｈｉｒｅの汚水処理施設が攻撃され、汚水が河川や公園に流入した事例である。この攻撃者は、標的とする施設の近隣に移動し、車内から盗んだ双方向の無線機とノートパソコンを用い、無線で管理システムに不正な命令を送信し、警報の解除、通信妨害、ポンプの機動や停止等を実施していた。２００３年１月には、米国のＤａｖｉｓ－Ｂｅｓｓｅ原子力発電所のコンピュータがＳＱＬ　Ｓｌａｍｍｅｒ（エスキューエル　スラマー）[3]というマルウェアに感染した。その結果、通信の過負荷により、安全監視システム等に５～６時間にわたってアクセスできなくなるという事案が発生した[4]。ＳＱＬ　Ｓｌａｍｍｅｒは、ＭｉｃｒｏｓｏｆｔのＳＱＬ　Ｓｅｒｖｅｒ[5]等の脆弱性を利用して自身を拡散させるだけの単純な機能を備えており、その感染動作が単純で自身のサイズも小さいことから、爆発的に感染台数を増やしたとされている。２００５年８月には、ドイツのダイムラー・クライスラー社[6]の１３の自動車工場において、各工場のシステムがオフラインとなり、生産が５０分間停止する事案が発生した。この事案では、外部から持ち込まれたパソコンにより、マルウェアに感染した可能性が指摘されている。２００６年８月には、南アフリカのＴｓｈｗａｎｅのＳＣＡＤＡ[7]システムが攻撃され、ＭａｍｅｌｏｄｉおよびＥｅｒｓｔｅｒｕｓｔにおいて１１日間水を得ることができない状態となった[8]。同じく２００６年８月には、米国のロサンゼルスで交通監視センターが不正アクセスを受け、４つの混雑する交差点の信号が使用できない状態とされた。２００６年１０月には、米国のＨ

---

[3]インターネット上でデータベースサーバを対象として感染を拡大するワーム

[4]Kevin Poulsen (2003). "Slammer worm crashed Ohio nuke plant network"

[5]データベースを提供するソフトウェア

[6]現在のダイムラー社

[7]SCADA (Supervisory Control And Data Acquisition) 汎用のコンピュータで動作する産業制御システムの一種であり、監視や制御を実施する。

[8]TNO Defence, Security and Safety (2008). "SCADA Security Good Practices for the Drinking Water Sector"

ａｒｒｉｓｂｕｒｇの浄水場のＳＣＡＤＡシステムがインターネット経由で不正アクセスを受けた。攻撃者は従業員のパソコンに遠隔操作のためのマルウェアをインストールして制御を奪った。その後、その従業員のパソコンを踏み台してＳＣＡＤＡシステムに侵入し、ＨＭＩ[9]にマルウェアをインストールする事に成功している。２００８年１月には、ポーランドで１４歳の少年が、テレビの遠隔操作機器のようなものを線路の切り替えができるように改造し、４台のトラムを脱線させるという事件が発生した[10]

このように、初期の制御システムへのサイバー攻撃は、不正な命令を実行したり、一般的なコンピュータへの共通の不正アクセスの手法を用いたりする単純なものであった。また、その動機についても個人的な反発や興味によるものがほとんどであった。その後、制御システムへの汎用のコンピュータやインターネットと同じ通信方式の普及に伴い、本格的な制御システムへのサイバー攻撃が懸念されるようになってきた。

（２）本格的な制御システムへのサイバー攻撃

本格的な制御システムへのサイバー攻撃の脅威が確認できたのは、２００７年３月に米国のアイダホ国立研究所で実施された「オーロラ発電機テスト」である。この実験では、ディーゼル発電機の制御プログラムを不正に操作することで、異常な振動と煙を発生させ、発電機を物理的に破壊することに成功している。２００８年８月には、トルコの石油パイプラインが爆発し、サイバー攻撃が原因であった可能性が指摘されている[11]。この事案では、監視カメラの通信ソフトの脆弱性を利用して内部ネットワークに侵入し、警報装置を停止させて管内の圧力を異常に高めて爆発を引き起こしたとの意見もある。そして２０１０年６月には、制御システムを狙った初のマルウェアであるＳｔｕｘｎｅｔ[12]（スタックスネット）が発見された。Ｓｔｕｘｎｅｔは米国とイスラエルが共同で開発し、イランの核燃料施設の遠心分離機を制御するコントローラの制御を奪い、約８４００台の遠心分離機を稼動不能に陥らせたと言われている。その後、２０１１年７月にはＤｕｑｕ[13]、２０１２年５月にはＦｌａｍｅ[14]、同６月にはＧａｕｓｓ[15]と呼ばれるＳｔｕｘｎｅｔの後継と考えられるマルウェアが発見されている。２０１２年に開催されたロンドンオリンピックでは、実際の被害は発生しなかったものの、オリンピック開会式の照明システムへのサービ

---

[9]HMI (Human-Machine Interface) オペレータの操作端末

[10]THALES (2016). "Ground Transportation Cybersecurity"

[11]SANS ICS (2014). "Media report of the Baku - Tbilisi - Ceyhan (BTC) pipeline Cyber Attack"

[12]Symantec (2011). "W32.Stuxnet Dossier"

[13]Symantec (2011). "W32.Duqu"

[14]Laboratory of Cryptography and System Security (2012). "sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks"

[15]Kaspersky (2012). "Gauss: Abnormal Distribution"

ス拒否攻撃が４０分間にわたって実施されたことが公表されている。さらに２０１４年には、欧米のエネルギー関係企業を標的とした、大規模な標的型攻撃が観測されるようになった。この攻撃者はＤｒａｇｏｎｆｌｙ[16]あるいはＥｎｅｇｅｔｉｃ　Ｂｅａｒ[17]と呼ばれており、Ｈａｖｅｘと呼ばれる制御システムを標的としたマルウェアを用いている。２０１４年８月には、米国のミシガン州の無線ＬＡＮを用いた信号システムに脆弱性があり、信号の操作が可能であることが確認された[18]。２０１４年１２月には、ドイツの製鉄所がサイバー攻撃を受け、溶鉱炉を正常に停止できなくなり、生産設備が損傷する事件が発生した。さらに２０１５年１２月には、米国のＢｏｗｍａｎ　Ａｖｅｎｕｅダムの管理システムが不正アクセスを受けていたことが発覚した。実際の不正アクセスは２０１３年であり、水門の制御が奪われた状態になっていたが、水門が保守作業で切り離されていたため、実際に開閉されることはなかったとされている。２０１６年３月には、米司法省はこのサイバー攻撃に関与したとされるイラン政府と関係する企業に所属する７名を起訴している。同じく２０１５年１２月には、ウクライナの複数の電力会社がサイバー攻撃を受け、推定１４０万世帯で停電が発生したとされている。攻撃者は、Ｂｌａｃｋ　Ｅｎｅｒｇｙ[19]と呼ばれるマルウェアを用いた標的型メール攻撃により認証情報を盗み出し、その認証情報を用いて監視制御システムに侵入し、ＨＭＩの制御を奪っている[20]。この攻撃ではＣｒａｓｈＯｖｅｒＲｉｄｅと呼ばれるマルウェアが用いられ、送電グリッドに障害が発生したとされている[21]。ＣｒａｓｈＯｖｅｒＲｉｄｅは電源スイッチやブレーカーを制御する機能を備えており、様々なプロトコルに対応しているため、より広範囲の攻撃に使用することも可能である。攻撃者はさらに、コールセンターの電話回線へのサービス拒否攻撃も実施しており、問い合わせによる発覚を遅らせることを目的とした可能性が指摘されている。攻撃者の正体については、Ｓａｎｄｗｏｒｍ　Ｔｅａｍと呼ばれるロシアのハッカー集団であるとされている[22]。やや本題とは外れるが、２０１４年にはＩｎｓｅｃａｍ[23]というサイトで世界中の初期パスワードをそのまま使用している無防備な監視カメラの映像が公開されていることが話題となった。このサイトでは、今も多数のカメラの映像がリアルタイムで公開されている。さらに２０

[16]Symantec (2014). "Dragonfly: Cyberespionage Attacks Against Energy Suppliers"
[17]Kaspersky (2014). "Energetic Bear - Crouching Yeti"
[18]Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman (2014). "Green Lights Forever: Analyzing the Security of Traffic Infrastructure"
[19]F-Secure (2014). "BLACKENERGY & QUEDAGH"
[20]SANS ICS (2016). "Analysis of the Cyber Attack on the Ukrainian Power Grid"
[21]Doragos (2017). "CRASHOVERRIDE Analyzing the Threat to Electric Grid Operations"
[22]iSIGHT Partners (2014). "Russian Cyber Espionage Campaign - Sandworm Team"
[23] https://www.insecam.org/

１７年４月には、米国のダラスの竜巻等の危険を知らせるための野外警報サイレンが、不正に鳴らされる事案が発生した。この事案では、警報システムの制御に利用される無線が悪用され、無線信号のリプレイ攻撃[24]を受けた可能性が指摘されている。このような攻撃は、ソフトウェア無線機や無線周波数のテスト機材を保有していれば、実行することが可能である。２０１７年８月には、中東の企業において制御システムが異常停止する事態が発生した。その後の調査によると、その原因は安全計装システムであるＴｒｉｃｏｎｅｘを狙ったＨａｔＭａｎ（あるいはＴｒｉｔｏｎ）と呼ばれるマルウェアであったことが判明した[25]。また、報道はほとんどされていないが、国内においてもマルウェアの感染により、自動車工場や半導体工場の生産ラインが停止したり、処理能力が低下したりする被害が報告されている[26]。

このように、近年ではサイバースペースから物理ドメインに干渉し、物理的な被害をもたらす本格的な制御システムへのサイバー攻撃が発生している。また、政府や情報機関が関与したと考えられる事例や、軍事作戦と協調した事例も確認されている。

３　制御システムの概要

（１）制御システムの基本動作

制御システムは、産業制御システム（ＩＣＳ[27]）あるいは監視制御システム（ＳＣＡＤＡ[28]）と呼ばれることもあり、他の機器やシステムを制御するための一連の機器あるいは機器群のことである。具体的には、エアコン、冷蔵庫、洗濯機等の家電から、自動車、エレベータ、電車、航空機、船舶等のビークル、電力、ガス等のエネルギー関係機器、製造・組み立て産業における工場の機器等が挙げられる。このように、制御システムは、多くの重要インフラを支えている。制御システムの基本動作を図１に示す。

---

[24]過去に発信された無線信号を記録してこれを再生する手法

[25] Fire Eye (2017). “Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure”

[26]IPA (Information-technology Promotion Agency) 情報処理推進機構

[27]ICS (Industrial Control System)

[28]SCADA (Supervisory Control And Data Acquisition) 汎用のコンピュータで動作する産業制御システムの一種であり、監視や制御を実施する。

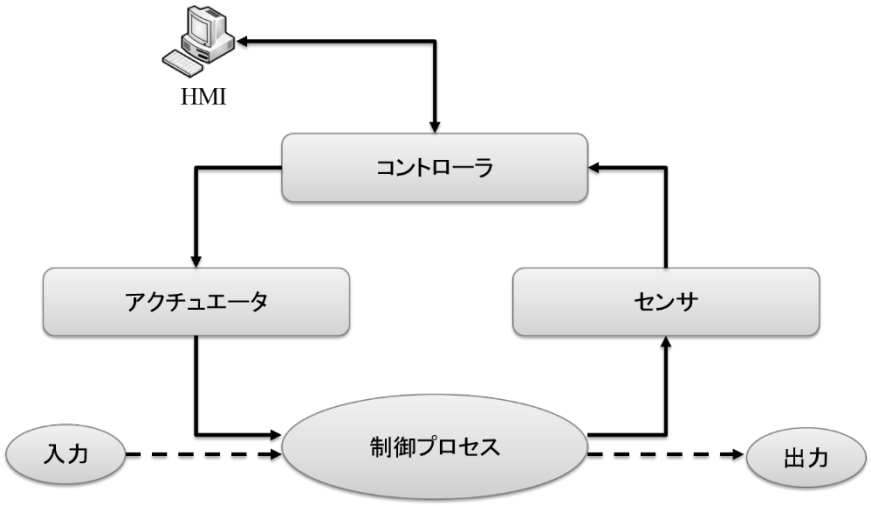

図１：制御システムの基本動作

何らかの入力に対して結果を出力する制御プロセスは、センサ、コントローラおよびアクチュエータを介して動作する。センサは音、光、温度、加速度等の物理特性を計測し、その情報を信号に変換してコントローラに送信する機器である。コントローラは、センサからの信号を解釈し、設定に基づいて操作を決定し、操作命令をアクチュエータに送信する。アクチュエータはバルブ、スイッチ、ブレーカー、モーター等のことであり、コントローラからの命令に従って制御プロセスを実行する。操作員、エンジニア等のオペレータは、ＨＭＩ[29]と呼ばれるパソコンや専用の端末を利用し、制御手順の入力、監視、パラメータの設定等を実施する。

これらの制御システムは、かつては独自仕様の機械や電子回路で構成されていたが、近年では利便性やコストの観点から、汎用のコンピュータやインターネットと同じ通信方式が採用されるようになってきた。そのため、情報システムと制御システムは、有機的に連接してネットワークを構成することが可能となった。

（２）ネットワーク構成

一般的な制御システムのネットワーク構成を図２に示す。

[29]HMI (Human-Machine Interface)

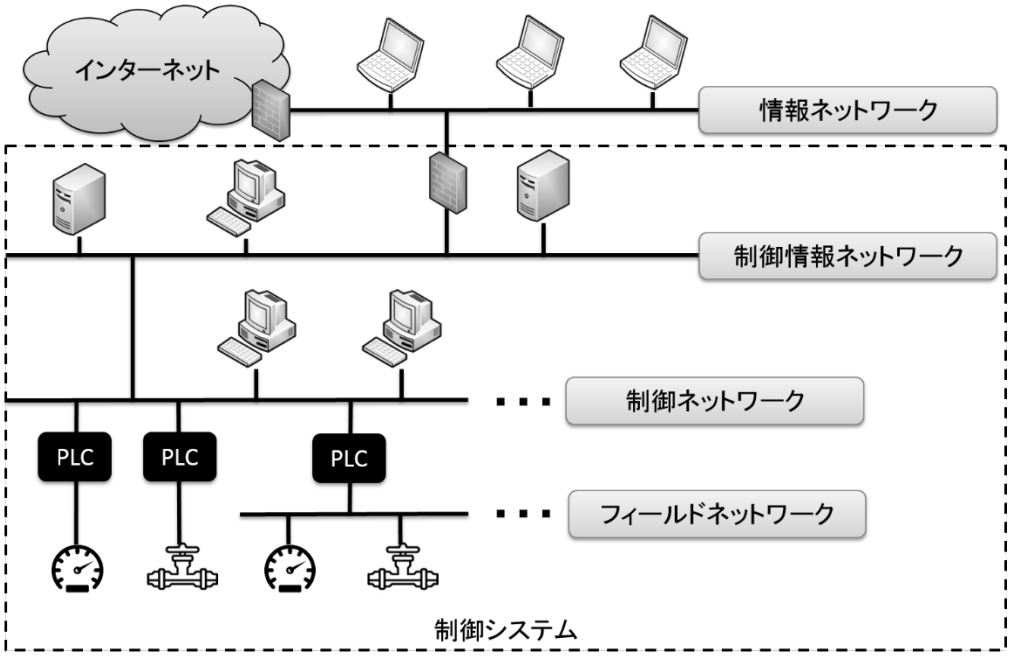

図２：一般的な制御システムのネットワーク構成

図中の情報ネットワークは、インターネットに接続するいわゆる一般的な情報システムのネットワークであり、事務等の業務に用いられる。その下に接続している制御情報ネットワークも、情報ネットワークと同様の方式で動作するネットワークである。ただし、制御情報ネットワークでやり取りされる情報は、制御システムの操作や計測された値の履歴、計画に関する情報等の制御情報となっている。制御情報ネットワークには、発注から生産完了までを管理する生産管理サーバ等が配置されている。さらにその下に接続する制御ネットワークには、ＰＬＣ[30]と呼ばれるコントローラが接続されている。制御ネットワークは、かつては分野や国によって独自の通信方式が用いられてきたが、近年ではインターネットと同じ通信方式が用いられることが多くなってきている。コントローラの下には、センサやアクチュエータ等の機器が接続されている。フィールドネットワークは、かつてはシリアル通信やパラレル通信が用いられてきたが、これも近年ではインターネットと同じ通信方式が用いられるようになってきている。しかしながら、インターネットと同じ通信方式では、即時性が求められる場合に対応できないことがある。そのため、即時性が求められる場合には、一般に何らかの高速化のための工夫が必要となる。

（３）制御システムの特徴

次に、制御システムを一般的な情報システムと比較した場合の特徴について考察する。制御システムの特徴を表１に示す。

表１：制御システムの特徴

[30]PLC (Programmable Logic Controller)

	情報システム	制御システム
サイバー攻撃の影響範囲	サイバースペースのみ	物理ドメインにも影響
対処の優先事項	機密性	可用性
運用停止	許容可能な場合が多い。	不可能の場合が多い。
機器や通信規約	標準	独自
保守の期間	３～５年	１０～１５年

情報システムでは、サイバー攻撃の直接的な影響範囲は基本的にサイバースペースのみである。ＤＤｏＳ[31]攻撃や標的型攻撃では、サービスの停止や情報漏洩のような論理的な被害は発生するが、直接的に物理的な被害が発生するわけではない。これに対し、制御システムでは、サイバー攻撃の影響範囲はサイバースペースだけに留まらず、物理ドメインにも直接的に影響する可能性がある。この点は、本稿の第２節の事例からも確認することができる。

制御システムと情報システムでは、サイバー攻撃が発生した場合の対処の優先順位も異なる。情報システムでサイバー攻撃が発生した場合には、サイバー攻撃の影響範囲を絞り込み、切り離す処置を実施する場合が多い。また、運用停止や再起動が許容される場合も多い。これに対し制御システムでは、継続して安全に稼動することが重視され、機器を直ちに停止することができない場合が多い。例えば、サイバー攻撃が発生した場合に、ただちにビークルの動作を止めたり、発電所や原子炉を急停止したりすることはできないであろう。また、重要インフラの停止は国民生活および社会活動に大きな影響を与えるため、実質的に運用停止が不可能である場合も多い。換言すると、情報システムでは機密性が優先される場合が多いのに対し、制御システムでは可用性が優先されることになる。

情報システムでは標準的な機器や通信規約が用いられているのに対し、制御システムでは機器や通信規約が独自の規格であることが多い。ただし、近年では制御システムの機器や通信規約についても、汎用のコンピュータやインターネットと同じ通信方式が採用されるようになってきている。

制御システムと情報システムでは、保守の期間についても異なる。一般に、情報システムでは３～５年程度の短期間で機器が入れ替わる。そのため、脆弱性の修正や対応は比較的容易である。これに対し制御システムでは、１０～１５年程度の長期間の保守が一般的であり、古い機器がいつまでも使用されている場合も珍しくない。そのため、脆弱性が発見されたとしても、修正や対応が困難である場合もある。

４　制御システムへのサイバー攻撃の仕組み

（１）制御システムへのサイバー攻撃の手順

制御システムへのサイバー攻撃の手順には、標的型攻撃との共通点が多い。

[31]DDoS (Distributed Denial of Service)

ＩＰＡ[32]が提唱する標的型攻撃の段階[33]を表２に示す。

表２：標的型攻撃の段階

段階		説明	サイバーキルチェーンの対応
1	計画立案	攻撃目標の選定 攻撃に必要な情報の収集 計画の立案	偵察
2	攻撃準備	攻撃に必要なインフラの準備 不正なコンテンツの作成	武器化
3	初期潜入	不正なコンテンツの送付あるいは ネットワーク経由で侵入	配送～攻撃
4	攻撃基盤構築	ＲＡＴ[34]のインストール 必要なツールのダウンロード等	インストール～ 遠隔操作
5	内部調査侵入	情報システム内部の調査 アクセス権の拡大等	侵入拡大
6	目的遂行	ＨＭＩのアクセス権の把握 制御システムの操作、破壊等	目的遂行
7	再侵入	必要に応じて再度侵入して調査	－

まず「計画立案」の段階では、攻撃目標を選定して必要な情報を収集し、計画を立案する。「攻撃準備」の段階では、Ｃ＆Ｃサーバ等の攻撃に必要なインフラを準備するとともに、マルウェア等の不正なコンテンツを作成する。「初期潜入」の段階では、何らかの物理的な手段で不正なコンテンツを標的に送付するか、あるいはネットワーク経由で制御システムに侵入する。「攻撃基盤構築」の段階では、端末を恒久的に遠隔操作するためにＲＡＴと呼ばれるマルウェアをインストールし、その後の「内部調査侵入」に必要なツール等をダウンロードする。「内部調査侵入」の段階では、情報システムの内部を調査してアクセス権を徐々に拡大し、「目的遂行」の段階では制御システムを操作するためにＨＭＩのアクセス権を把握し、制御システムの操作、破壊等を実施する。他の良く知られた標的型攻撃を段階的に区分したモデルとしては、ロッキード・マーティン社が提唱した[35]サイバーキルチェーン[36]が知られている。表２の右端は、ＩＰＡの各段階に対応するサイバーキルチェーンのプロセスを示している。

[32]IPA (Information-technology Promotion Agency) 情報処理推進機構
[33]情報処理推進機構(2014). 「「高度標的型攻撃」対策に向けたシステム設計ガイド」
[34]RAT (Remote Access Trojan or Remote Administration Tool)
[35]Hutchins, E.M. et al. (2009). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
[36]標的型攻撃の段階を連鎖的に偵察、武器化、配送、攻撃、インストール、遠隔操作、目的実行に区分したモデル

制御システムへサイバー攻撃を実施するためには、初期潜入のための侵入経路をみつける必要がある。侵入経路を把握していない場合には、標的とする組織や個人に標的型攻撃等を実施し、リモートメンテナンスのためのアクセス先、認証情報等の必要な情報を窃取する。あるいは、ソーシャル・エンジニアリング[37]を駆使して実地調査を実施し、物理的な手段、近距離からの無線ＬＡＮへのアクセスによる侵入経路等を調査する。

（２）制御システムへの侵入経路

制御システムは、セキュリティ対策の一環として、インターネットからアクセスする手段が制限されていたり、ファイアウォール等により情報ネットワークとも分離されていたりすることが多い。したがって、制御システムに侵入するためには、物理的な手段でマルウェア等を送付するか、制限されたネットワーク経由で侵入することになる。これまでの事例を分析すると、制御システムへの主な侵入経路は大まかに表３に示すとおりに整理できる。

表３：制御システムへの主な侵入経路

概要	侵入経路	
マルウェアに感染したＵＳＢメモリのパソコンへの挿入	ＵＳＢメモリ	物理的手段
保守等のために持ち込んだパソコン等がマルウェアに感染	パソコン	
リモートメンテナンスのためのＶＰＮ[38]接続により侵入	メンテナンス用の回線	ネットワーク経由
無線ＬＡＮの脆弱性等を利用して侵入	無線ＬＡＮ	

ＵＳＢメモリとパソコンは、物理的な手段でマルウェア等を持ち込むことに該当する。制御システムはインターネットへのアクセスが制限されることが多い。そのため、修正プログラムの適用等のメンテナンス作業のため、ＵＳＢメモリを使用してデータのやり取りを実施することは珍しくない。また、保守等のためにメンテナンス用のパソコンを持ち込む場合もある。このような外部から持ち込まれたＵＳＢメモリやパソコンには、マルウェア等の不正なプログラムが混入している可能性がある。これらは、内部犯やメンテナンス業者によって意図的に持ち込まれる場合もあれば、感染に気づかずに持ち込まれてしまう場合もあり得る。

メンテナンス用の回線と無線ＬＡＮは、ネットワーク経由で侵入することに該当する。メンテナンス用の回線は、インターネットを経由したＶＰＮによっ

[37]人間の行動や心理の特徴を悪用して機密情報等を入手する手法を指す。
[38]VPN（Virtual Private Network）インターネット上に仮想的に構成する専用回線

て構成されていることがある。この場合、そのＶＰＮアプリケーションと認証情報を入手すれば、第３者がインターネット経由でアクセスできる可能性がある。あるいは、メンテナンスを実施する個人の端末の制御を奪うことができれば、その端末の踏み台にして制御システムにアクセスすることができる可能性がある。また、制御システムで無線ＬＡＮを用いている場合には、その脆弱性をついて通信内容を盗聴したり、任意の命令を実行したりすることができる可能性がある。無線ＬＡＮの脆弱性としては、通信を暗号化していない場合、ＷＥＰ[39]等の古いプロトコルを使用している場合、容易に推測可能なパスワードを使用している場合、設定に不備がある場合等が考えられる。

（３）目的の遂行

一般的な情報システムと制御システムの違いは、制御システムにはコントローラ、アクチュエータおよびセンサが存在することである。アクチュエータはサイバースペースの情報を物理現象に変換し、サイバースペースから現実世界への出口の役割をはたす。センサは逆に、物理現象を論理的な情報に変換し、現実世界からサイバースペースへの入口の役割をはたす。そして、コントローラは出入口であるアクチュエータとセンサを制御する。つまり、物理ドメインへの干渉という制御システムの重要な特性の要となっているのは、コントローラである。コントローラには、通常はＨＭＩからアクセスする。したがって、攻撃者がＨＭＩの制御を奪った場合には、制御システムを物理的に操作できる状態になったことを意味する。換言すると、制御システムへのサイバー攻撃の場合、攻撃者の目標はＨＭＩ制御を奪うことである。その後、攻撃者はＰＬＣの脆弱性をついて攻撃することも可能である。実際に、工場の生産ラインや化学プラントで使用されるＰＬＣの脆弱性や、実際に攻撃に利用することができる実証コードも公開されている。

制御システムへの別の攻撃手法としては、サイバースペースへの入口であるセンサからの攻撃が考えられる。例えば、センサであるマイク、カメラ、アンテナ等に細工をした音声、画像、電波等を入力し、変換された信号を処理する過程に脆弱性があった場合、コントローラを誤動作させることができる可能性がある。２０１１年にイラン領内に米国の無人機が着陸した事件では、偽のＧＰＳ信号により制御が奪われた可能性が指摘されている。このような物理空間からの攻撃に対しては、センサセキュリティあるいは計測セキュリティという分野で対策が検討されている。

５　サイバー攻撃への対策

（１）物理的対策

制御システムへのサイバー攻撃の対策として第一に挙げられるのは、物理的

---

[39]WEP（Wired Equivalent Privacy）初期の無線 LAN の脆弱なプロトコルの１つであり、第３者が容易に通信内容を解読することが可能である。

手段による侵入経路での対策である。特に、インターネットから分離された制御システムにおいては、ＵＳＢメモリや保守用に外部から持ち込まれたパソコンが主要な感染経路となっている。したがって、これらのＵＳＢメモリやパソコンの管理を適切に実施することが重要である。

ＵＳＢメモリに関しては、私有のＵＳＢメモリの使用を禁止し、利用可能なＵＳＢメモリを最低限度に制限することで、不正なプログラムの流入のリスクを減らすことができる。制御システム側においても不要なＵＳＢポートは閉鎖し、マルウェアが感染の際に悪用する自動実行の機能を無効化する等の対策が必要である。また、ＵＳＢメモリの挿入時には、最新のウイルス定義ファイルを用いてウイルスチェックを行う等の対策は最低限必要である。ＵＳＢポートに関しては、物理的な手段の他にも、ＯＳ[40]の機能や専用の管理ソフトウェアを用いて論理的に無効化することも可能である。また、自動実行の機能の無効化も、ＯＳで設定することが可能である。

パソコンに関しても同様に、私有のパソコンの持ち込みを禁止し、持ち込まれるパソコンを最低限度に制限することで、不正なプログラムの流入のリスクを減らすことができる。端末の入れ替えや保守用の端末を持ち込む場合には、最新のウイルス定義ファイルを用いてウイルスチェックを行う等の対策は最低限必要である。

これらの対策を適切に実施したとしても、ウイルス対策ソフトでは検知できない未知のマルウェアやゼロデイ攻撃[41]は検知することはできない。また、人為的なミスや内部犯により、チェックをしていないＵＳＢメモリやパソコンが持ち込まれてしまう可能性はある。したがって、このようなチェックが機能しなかった場合も想定し、多層防御の考え方でセキュリティ対策を検討する必要がある。

（２）ネットワークにおける対策

ネットワーク経由の侵入経路における対策としては、適切なアクセス制御とネットワークの監視が主要な対策となる。

リモートメンテナンスのための回線については、接続できる端末を認証するとともに、アクセス元についても制限すべきである。これにより、攻撃者が回線にアクセスする難易度を高めることができる。さらに、メンテナンス回線のアクセスの履歴をチェックし、心当たりのない不審なアクセスがないか定期的に確認することが重要である。

無線ＬＡＮに関しては、制御システム内部での活用には大きなリスクがあることを認識し、やむを得ず活用する場合には適切にセキュリティ対策を実施する必要がある。

ネットワークにおける対策についても同様に、適切なアクセス制御を実施し

---

[40]OS（Operating Software）

[41]修正プログラムが公開されていない未知の脆弱性を用いた攻撃であり、ＯＳやアプリケーションを最新の状態に更新していても防ぐことができない。

たとしても不正アクセスを受ける可能性はある。例えば、標的型攻撃によりメンテナンスのための認証情報が窃取され、さらに担当者の端末が遠隔操作された場合には、攻撃者は正当な手段でメンテナンス回線にアクセスすることができてしまう。また、内部犯やソーシャル・エンジニアリングによりアクセス制御が突破される可能性もある。したがって、制御システム内部のネットワークについても用途に応じて区分し、適切にアクセス制御を実施することが重要である。さらに、ネットワーク内部を監視し、ログ管理ツールや専用の機能を用い、不審な通信がないか確認することが重要である。

（３）修正プログラムの適用

制御システムへのサイバー攻撃では、様々な脆弱性が悪用されている。したがって、ＯＳやアプリケーションの修正プログラムは可能な限り速やかに適用することが重要である。

しかしながら、制御システムはインターネットから分離されていることも多いため、分離されているから安全だという思い込みがある。また、ＵＳＢメモリ等の物理的な手段を用いる必要もあり、修正プログラムの適用にも手間がかかる。そのため、修正プログラムに関しては、適用が見送られてしまう場合も珍しくない。また、制御システムには、専用のアプリケーションが用いられることも多い。そのため、仮に修正プログラムを適用しようとしたとしても、正常な動作が保証されない可能性がある。したがって、修正プログラムの適用にあたっては、事前に検証環境において正常な動作を確認することが重要である。このような検証は、ベンダの協力がなくては対応が難しい事項である。そのため、サイバー攻撃発生時の対応も含め、契約時にしっかりとセキュリティに関する項目を取り決めておくことが重要である。

制御システムにおいては、対処においても可用性が重視され、運用の停止が許容されない場合も考えられる。そのような場合、定期メンテナンスや操業停止の期間を考慮し、計画的に修正プログラムを適用する必要がある。どうしても適用が難しい場合には、アクセス制御を実施したり、監視を強化したりする等、何らかの緩和策を検討すべきである。

６　おわりに

本稿では、制御システムへのサイバー攻撃とその対策をとりあげた。第２節では、実際に物理的な被害をもたらした制御システムへのサイバー攻撃の事例を取り挙げ、その脅威と重要性について説明した。第３節では、制御システムの基本動作、ネットワーク構成およびその特徴について、情報システムの違いを中心に説明した。第４節では、制御システムへのサイバー攻撃の手順、侵制御システムへの侵入経路および目的の遂行について、標的型攻撃と比較しながら要点を説明した。第５節では、制御システムへのサイバー攻撃に対する基本的な対策について説明した。

制御システムへのサイバー攻撃は、物理ドメインに干渉するという極めて重

要な特性を持っている。また、国民生活および社会活動に不可欠な重要インフラは、制御システムによって支えられている。したがって、制御システムへのサイバー攻撃の対策は、国家の安全保障に不可欠な要素である。すでに、制御システムへのサイバー攻撃により、制御システムの物理的な破壊、大規模な停電等の伴う事件が発生している。また、国内においてもマルウェアにより制御システムが停止し、実際に工場の生産が停止する事案が発生している。さらに、制御システムを明確に標的とする高度なマルウェアや、国家の関与が疑われる事案も確認されている。制御システムの物理的な破壊や停電は、実際の軍事作戦に対しても極めて大きな影響を与える可能性が高い。これらのサイバー攻撃は、実際の軍事作戦と協調して実施されている。したがって、制御システムへのサイバー攻撃の脅威と重要性については、国家の安全保障に携わる者が認識しておくべきである。また国家としてその対策を推進しなければならない。本稿で紹介した対策は、あくまでのどの組織においても実行できることを想定した最低限の対策である。このような基本的な対策を徹底することにより、多くの既知のサイバー攻撃を防ぐことは可能である。しかしながら、Ｓｔｕｘｎｅのように複数の未知の脆弱性を利用し、国家が主体となった本格的なサイバー攻撃を防ぐことは難しい。国民生活および社会活動に不可欠な重要インフラについては、多層防御による高度なサイバー攻撃への対策が必要である。２０１７年には、ＩＰＡの内部に産業サイバーセキュリティセンターが発足し、政府においても重要インフラのサイバー防衛での安全基準の策定が開始された。国家の安全保障のために適切な基準を策定し、どのように運用し、これを維持管理していくかが今後の課題である。