産業用制御システムのセキュリティについて

今年 7 月に欧米フィアット・クライスラー・オートモービルズが自動車の運転制御システム乗っ取りを防ぐために 140 万台のリコールを発表した。また 8 月にアメリカ・ラスベガスで開催された情報セキュリティの国際大会「ブラックハット」でアメリカの研究チームが「発電所や工場に使う制御システムの通信装置に重大な脆弱性を発見した」と報告する等、制御システムのセキュリティ対策の重要性が高まっている。

そこで本稿では、産業用制御システムのセキュリティについて、一般社団法人 JPCERT コーディネーションセンター 制御システムセキュリティ対策グループ マネージャ 中谷 昌幸氏に解説いただいた。

1. 産業用制御システム（ICS：Industrial Control System）について

独立行政法人情報処理推進機構（IPA）が発行する「重要インフラの制御システムセキュリティと IT サービス継続に関する調査」[1]では、「制御システムは、他の機器やシステムの動作を管理、指示、制御するシステムであり、センサーやアクチュエーターなどのフィールド機器、制御用ネットワークコントローラー、監視・制御システム（SCADA : Supervisory Control And Data Acquisition とも呼ばれる）などで構成されている。」と定義されている。以下では、産業用制御システムを「制御システム」として表記する。

制御システムは、利用される分野が多岐にわたり、電力やガスといったエネルギー産業に始まり、自動車や家電などを製造する製造業、荷物の輸送を行う物流業など多くの産業分野で使用されている。制御システムは、FA（Factory Automation）系の制御システムと PA（Process Automation）系の制御システムに分けることができる。前者は主に自動車や電機などの部品を組み立てて製品を製造するようなシステムで、後者は電気やガス、石油化学製品などを生産するシステムを指す。この他に、ビルの空調や照明などを制御するビル制御システム（BA : Building Automation）といったものもある。このビル制御システムまで含めると、制御システムはほとんどの産業分野に関わるシステムであると言えるかもしれない。

工場の設備が自動化されはじめた 1970 年代の制御システムは、主に製造ベンダーが独自に開発した技術を中心に構成されていた。このため、当時の制御システムの多くは、他社の製品との相互接続性はほとんど備えていなかった。加えて、当時の制御システムは地理的に離れた他の地

[1] https://www.ipa.go.jp/files/000013981.pdf

域のシステムと連携するネットワーク機能は備えていなかった。

その後、情報システムがオープン化したのと同様に、1990 年代以降には制御システムにもオープン化の波が訪れた。SCADA や DCS（Distributed Control System）で使用される HMI（Human Machine Interface）といった人間が操作する端末には、米 Microsoft 社の Windows OS が採用され、それらとの通信規格には Ethernet と TCP/IP プロトコルといったインターネットの技術が使用されるようになった。加えて、企業活動がグローバル化し、複数の工場や企業間の連携により製品を製造するようになった結果、工場と工場の間が専用線やインターネットなどのネットワークでつながるようになったり、生産計画を元にタイムリーに製品製造を行うために、工場の制御システムと本社の情報システムが連携するといった構成が取られるケースも増えてきた。

このような進歩・進化をたどった結果、制御システムの機能は飛躍的に向上していった。しかし、その一方で情報システムにおいて発生していたコンピュータウィルスなどの脅威の流入という弊害も発生するようになっていった。

また、制御システムの運用面での大きな特徴として、システムの可用性に重点が置かれていることがあげられる。情報セキュリティは、情報の「機密性（Confidentially）」、「完全性（Integrity）」、「可用性（Availability）」を維持することと定義されており、一般的に情報システムでは「機密性」が最も重要な要素と位置づけられているが、制御システムでは工場の連続稼働が企業の生産性に直結することから、「可用性」が最も重要な要素と位置づけられている。

2. 制御システムへの脅威

（1）情報システムへの脅威

制御システムへの脅威について触れる前に、情報システムへの脅威について少し触れてみたい。

企業活動において IT やインターネットの活用が当たり前のようになった現在、IT やインターネットを中心として構成される情報システムはサイバー攻撃の脅威にさらされることとなった。

インターネットが加速度的に普及を始めた 2000 年前後における脅威は、スクリプトキディといわれる愉快犯や自身の能力の証明を目的としたハッカー（クラッカー）によるものが中心であった。その後、インターネットが社会に広く浸透し、オンラインバンキングやオンラインショッピングのようにインターネットを介して商取引が行われるようになった結果、金銭の窃取を目的とした攻撃者が出現し、そしてその数は急速に増加していった。

さらに、2000 年代後半には企業の知財や個人情報などの窃取を目的として、執拗に攻撃を仕掛けるいわゆる「標的型攻撃」といわれる攻撃が発生しだした。標的型攻撃は、攻撃者が目的を遂行するまで継続して行われる。一時的に攻撃を退けても攻撃者は執拗に攻撃を仕掛けてくるため、いつかは防御の間隙をついて攻撃が成功してしまう可能性がある。

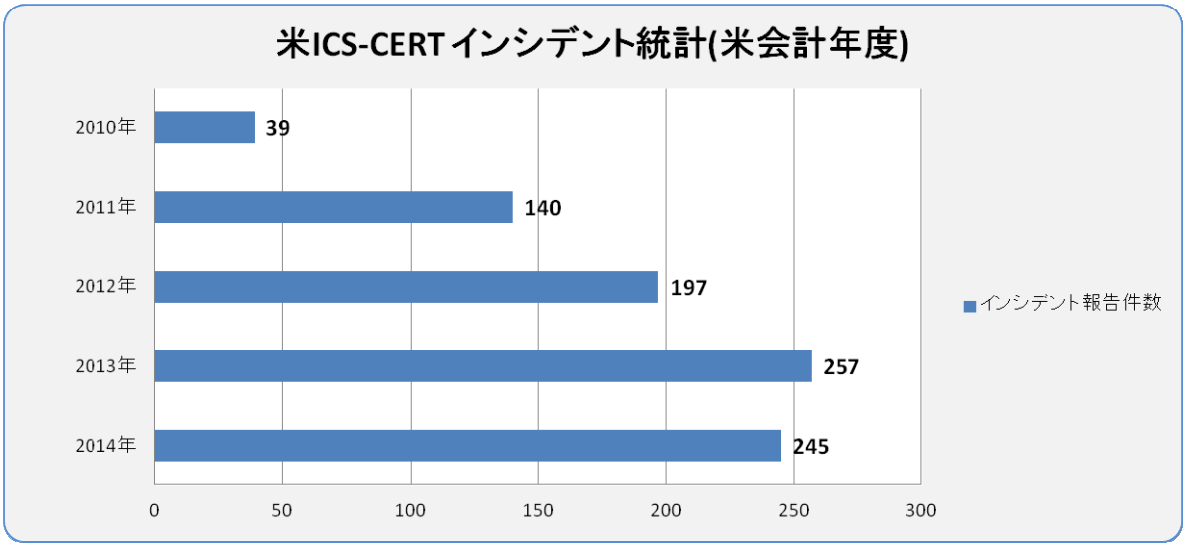
（2）制御システムへの脅威

一方の制御システムへの脅威については、実はその実態はあまり知られていない。

JPCERT/CC では、情報システム、制御システムの両方のセキュリティ事故（以降、「インシデント」とする）に関する報告の受付を行っており、情報システムについては月に 1,000 件を超える報告を受けている一方、制御システムに関する報告はほとんど受けていない。また、JPCERT/CC が 2013 年に国内の制御システムオーナー300 社にアンケート調査を行ったところ、およそ 7%の事業者から「コンピュータウィルスの感染被害経験がある」という回答[2]があった。

海外ではどうだろうか。米国では、制御システムのセキュリティ対策を専門に担う組織として、2009 年に国土安全保障省のもとに ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）が設立された。その ICS-CERT に報告されたインシデント報告件数を図 1 に示す。

■図 1　米 ICS-CERT におけるインシデント統計推移（米会計年度）



出典：「ICS-CERT Year in Review - 2014[3]」のデータをもとに筆者作成

[2] http://blog.jpcert.or.jp/2014/03/ics-security-conference-2014.html
[3] https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2014_Final.pdf

ICS-CERT には比較的多くの制御システムに関するインシデント報告が届いているが、それでも情報システムのインシデントに比べると 2 桁以上少ない数である。この要因としては、制御システムはインテグレーターやベンダーがインシデントを含めた保守対応を行っているためインシデント情報が外部に出づらいことや、制御システムへの攻撃の対価として金銭などの利得を得るビジネススキームが存在していないことが主たる要因ではないかと考えられている。

では、具体的にどういったインシデントが発生しているのだろうか？表 1 に海外でこれまでに発生した主な制御システム関連のインシデントを示す。

■表 1　主な制御システムに関連するインシデント

発生時期	発生地域	インシデント内容
2000 年	オーストラリア	解雇された元従業員が下水処理施設に対して不正アクセスを行い、処理設備を不正操作した
2003 年	アメリカ	原子力発電所の制御システムが SQL Slammer ワームに感染し、監視システムが一時的に停止した
2003 年	アメリカ	鉄道会社の信号や給電を制御するシステムが MSBlaster ワームに感染し、鉄道の運行に影響が生じた
2005 年	アメリカ	自動車メーカの制御システムネットワークに Zotob ワームが侵入し、工場の組立ラインが停止した
2009 年	アメリカ	元従業員が過去に貸与されたリモートアクセス権を使用し、電力会社のシステムに不正アクセスした
2009 年	オーストラリア	配電小売事業者の社内ネットワークにワームが侵入し、多数の端末が感染し、電力系統にまで影響が及ぶ可能性があった
2010 年	イラン	ウラン濃縮施設が制御システムを狙う Stuxnet[4]ワームに感染し、濃縮用遠心分離機が不正操作された
2011 年	ブラジル	発電所システムが Conficker ワームに感染し、発電システムが稼働停止となった
2011 年	アメリカ	鉄道会社のコンピュータがハッカーの攻撃を受け、2 日間にわたって列車の運行に混乱が生じた
2012 年	アメリカ	Ugly Gorilla と呼ばれる攻撃者によるガスおよび電力システムを狙ったサイバースパイ活動が確認された
2012 年	サウジアラビア	国営石油会社の 3 万台にのぼるワークステーションがコンピュータウィルス感染による被害を受けた
2013 年	メキシコ、他	海上の石油掘削基地で、コンピュータウィルス感染によりコンピュータ網が停止
2014 年	ドイツ	製鉄所に標的型攻撃が行われ、攻撃者は内部システムに侵入後、生産設備を攻撃

出典：各種公開情報をもとに筆者作成

この表からも分かるように、制御システムで発生している主なインシデントは、情報システムで感染を広げるコンピュータウィルスの流入や内部犯行によって引き起こされるものが中心で、Stuxnet のような制御システムを狙ったコンピュータウィルスは非常に限定的であった。しかし、2014 年に米国および欧州において制御システムを標的とした 2 件のサイバー攻撃が発生した。

[4] Stuxnet：イランのウラン濃縮施設を攻撃するために作成されたコンピュータウィルス。制御システムを標的として作成された初のコンピュータウィルスと言われている。

これまでの制御システムにおけるサイバー攻撃は、政治的な意味合いを持つと言われるStuxnetという特異なコンピュータウィルスを除き、情報システムで流行したコンピュータウィルスがたまたま制御システムにも感染を広げたケースがほとんどであった。しかし、2014年にはとうとう制御システムを標的とした攻撃が発生した。

その一つは、Havex RATといわれるコンピュータウィルスを使用した攻撃で、攻撃者は制御システムの関係者が閲覧するWebサイトを乗っ取り、そこにコンピュータウィルスを仕込むことで、エンジニアのコンピュータにコンピュータウィルスを感染させ、制御システムネットワーク内に侵入することを目論んだものであった。もう1つは、BlackEnergy2と言われる攻撃で、インターネットに接続されたHMIのソフトウェアの脆弱性をついて、感染するコンピュータウィルスを使用した攻撃であった。

これらの攻撃の特徴の1つとして、攻撃者は標的に対して金銭を要求したり、破壊活動といった行為を行わず、ひっそりと制御システムの情報を窃取することがあげられる。攻撃者の真意は定かではないが、重要インフラの制御システムへの攻撃は背後に国家規模のスポンサーがいて、有事の際に相手国にダメージを与える事を目的としているのではないかと言われていることから、これらの攻撃は事前の偵察活動ではないかという説が出ている。

また、表1で示したように制御システムがサイバー攻撃によって被害を受けた場合、実社会に直接影響を与えるような事態を引き起こすケースがある。加えると、制御システムの制御対象である機器（ポンプ、タンク、モーターなど）に影響を与えるような攻撃であった場合、最悪の場合物理的損壊にまで被害が及ぶ可能性を秘めている。このため、制御システムのセキュリティはインシデントの発生数が少ないからといって軽視できない重要な問題である。

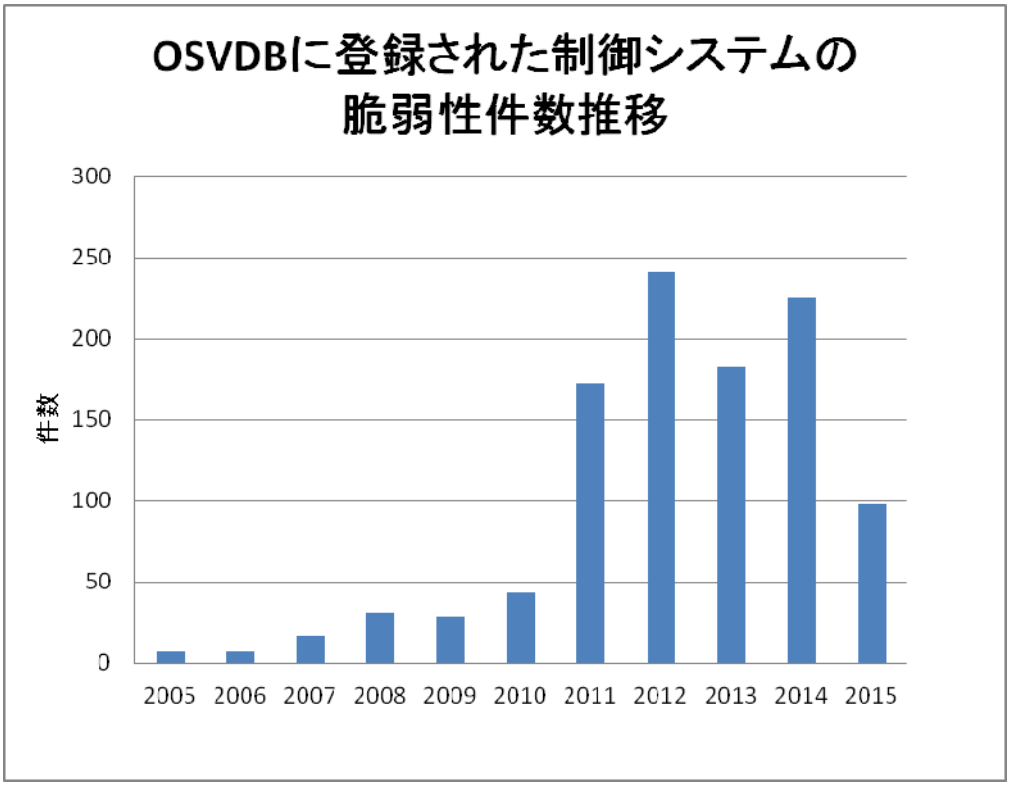
（3）制御システムソフトウェアの脆弱性

一般的にソフトウェアの欠陥である「脆弱性」は、主にセキュリティの研究者によって調査・検出され、ベンダーにその情報が提供される。ベンダーは、提供された情報を元に脆弱性を修正したソフトウェアを作成し、ユーザーに提供する。

情報システムのソフトウェアでは、脆弱性が年間1万件前後発見されており、攻撃者はソフトウェアの脆弱性を悪用することで攻撃対象のシステムに不正アクセスすることを目論んでいる。一方の制御システムソフトウェアの脆弱性も昨今発見されはじめた。図2にOSVDB（Open Source Vulnerability Database）[5]の脆弱性データベースから作成した制御システム関連ソフトウェアの脆弱性件数の推移を示す。

[5] http://osvdb.org/

■図 2　OSVDB に登録された制御システムの脆弱性件数の推移



出典：OSVDB（Open Source Vulnerability Database）の脆弱性データベースをもとに筆者作成

図 2 のように、制御システムでは 2010 年の Stuxnet の発現によりセキュリティに注目が集まって以降、毎年 200 件前後の脆弱性が発見されている。ただし、これもインシデント報告件数と同様に情報システムの脆弱性件数と比べると 2 桁以上少ない。これは、制御システムの脆弱性を調査している研究者が情報システムを調査している研究者に比して少ないためであり、現在発見されている脆弱性は氷山の一角であると言われている。

前述のように、制御システムは可用性が最重視されることから、製品ベンダーがこれら脆弱性を修正したプログラムを作成・配布したとしても、それを適用するためにシステムを即時停止させることは困難である。通常このようなシステムの停止を伴うメンテナンスは短くて半年、一般的には数年に 1 回の頻度でしか行われないため、それまでの間システムは脆弱な状態で運用されているのが現状である。

3. 制御システムのセキュリティ対策について

制御システムは可用性を重視する特質から、システムの再起動などが必要となるソフトウェアの修正プログラムの適用は難しい。また、一部の制御システムはリアルタイム制御と言われるミリ秒単位の制御を行うシステムもあり、システムの処理時間に影響を与えうるウィルス対策ソフトは導入が困難である。

加えて、システムの長期利用という側面もある。一旦構築された制御システムは数十年にわたって利用され続ける。多くの場合、数年単位で定期改修が行われるため、そのタイミングで修正プログラムを適用したり、置き換え可能な一部のシステムの更新が行われる事があるが、それ以外のタイミングでセキュリティのためにシステムに手を加えることは稀である。その結果、OSを中心としたソフトウェアのサポート期間が終了しても、継続して使用され続けるケースも少なくない。

これらの理由から、制御システムはコンピュータウィルスを中心としたサイバー攻撃に非常に弱い側面を持っている。

このため、多くの制御システムではいわゆる「入り口対策」と言われるファイアウォールなどのゲートウェイセキュリティの導入やUSBメモリーなどの可搬メディアの使用を制限することで、一定のセキュリティレベルを確保している。

これらの対策の徹底により一定の成果は見込めるだろうが、前述したような制御システムを狙ったサイバー攻撃はこのような通常のセキュリティ対策では防ぐことが困難である。そこで、現在議論されているのが事故前提のセキュリティ対策である。

セキュリティインシデントは必ず発生するものとして、インシデントが発生した場合に、いかに被害を最小限にとどめるかといった点に重点を置く対策である。具体的には、社内に緊急対応のためのチーム（CSIRT：Computer Security Incident Response Team）を配置し、必要なリソース(人員、機材など)、権限を割り当てる。こういったCSIRTを設置する流れは情報システムを有する企業で一般化しつつあり、この流れが制御システムを有する企業にも波及することが期待される。

最後に、欧米では制御システムのセキュリティ対策をいかに効果的に実施していくべきかといった議論が行われており、国内でも一部で同様の議論が始まっている。今後、制御システムに対する脅威が拡大していく前に、できる限りの対策を施し、被害を未然に防ぐ、または拡大しないような対応体制が個社に広く浸透していくように、JPCERT/CC でもそれら活動を支援していきたいと考えている。

［2015 年 9 月 7 日発行］

【筆者紹介】

中谷 昌幸（なかたに まさゆき）

一般社団法人 JPCERT コーディネーションセンター

制御システムセキュリティ対策グループ マネージャ

2005 年より JPCERT コーディネーションセンターにおいて、早期警戒業務に従事。2009 年より、同グループマネージャとして、注意喚起、早期警戒情報などの情報発信から緊急対応までの業務を担当。2014 年からは、制御システムセキュリティ対策グループマネージャとして、制御システムセキュリティに関する普及啓発、情報発信などの業務を行っている。

http://www.tokiorisk.co.jp/

東京海上日動リスクコンサルティング株式会社

経営企画部・企画ユニット

〒100-0005 東京都千代田区丸の内 1-2-1 東京海上日動ビル新館 8 階

Tel.03-5288-6595 Fax.03-5288-6590

