PwC's Cyber Intelligence

危機に瀕する日本のICSセキュリティ
狙われるPLC

攻撃の標的となる日本のICSセキュリティ

産業用制御システム（ICS）セキュリティに対する脅威が近年、特に高まっています。直近の事案として、イランとイスラエルにおける制御システムにサイバー攻撃が発生し、国家安全保障に対する攻撃の一部であったと報道されています（※1）。また、米国の産業制御システムサイバー緊急事態対応チーム（ICS-CERT）のアドバイザリー件数は、2010年に18件だったのが2019年には231件と約13倍に増加しました。また2019年のICSへの攻撃は、2018年と比較すると2,000パーセント増という異常な伸びを見せました（※2）。これまでもICSセキュリティは重要な課題でしたが、現在はより深刻さを増し、重要度が高まっていると言えるでしょう。その脅威はサイバー攻撃によって社会や経済に深刻な被害をもたらすものとなっています。

2018年ごろからBlack Hatをはじめとするサイバーセキュリティカンファレンスでも、ICSセキュリティに関する発表が増加しています。日本企業およびその製品もターゲットとなっていますが、残念ながら国内の多くの企業は、依然ICSセキュリティへの危機意識は薄くICSを狙う攻撃グループの実態を理解しきれていないと言わざるを得ず、格好の標的になっている可能性があります。

深刻な被害をもたらすICSへのサイバー攻撃、その手口とは

近年、一際注目を集めたのはTRITONと呼ばれる攻撃フレームワークです（※3）。2017年、このサイバー攻撃によって石油化学プラントが停止しました。ターゲットになったのは重電メーカーの安全計装システム（SIS：Safety Instrumented System）の脆弱性でした。同社のPLC（Programmable Logic Controller：工場などの機械を自動的に制御する装置）は数多くの日本の企業で使用され、SISについては世界中のプラントで採用されているシステムであることから、その脅威は深刻です。

あるセキュリティ企業の報告によると、2019年の段階でHEXANE、PARISITE、WASSONITEなど11の攻撃グループが活動しており、その脅威は米国とアジア・太平洋地域で増大し、日本もターゲットに含まれています（※4）。

報告によればITシステムとOTシステムをブリッジして侵入するもの、リモートアクセスの際に利用するVPN（Virtual Private Network）の脆弱性を突くもの、サプライチェーンを狙うものなどさまざまな攻撃手法が確認されています。ITシステムとOTシステムがネットワークで結ばれているシステムが増えていることから、この2つをブリッジして攻撃を行う手法が特に広がっています。

出典

※1 National Cyber Directorate head: Cyber winter is coming

※2 X-Force Threat Intelligence Index2020（IBM Security）

※3 Triton is the world's most murderous malware, and it's spreading（2019年3月5日、MIT Technology Review）

※4 2019 YEAR IN REVIEW: The ICS Threat Landscape and Activity Groups(Dragos)

※5 BRIDGING THE IT AND OT CYBERSECURITY DIVIDE（Dragos）

pwc

各国のセキュリティ基準を満たさない製品は排除されるのか

こうした攻撃の激化に対して、米国や欧州を中心として対策が本格化してきています。これは同時に、米国が2019年に一部の外国製通信機器の締め出したように、安全保障上のセキュリティ問題のある製品の排除につながります。今後の購買や調達において一定の基準を満たさない製品やサービスは不利な立場になり、排除されることが予想されます。

米国ではNIST（国立標準技術研究所）が2015年に「産業用制御システム（ICS）セキュリティガイド」SP800-82Rev2を、2017年にセキュリティ基準SP800-171を公開しました。米国政府機関と取引するために、企業にはSP800-171への準拠が求められることになりました。

この基準では米国政府が定める機密情報以外の重要情報（CUI：Controlled Unclassified Information）を扱う企業や研究機関が対象になります。CUIにはヘルスケア情報や通信基地局の通信データなど、広範なデータが含まれ、ヘルスケア情報を保有する医療施設や貴重な研究データのある研究施設もこの対象となります。また、重要インフラの設備情報も対象となっており（ICSに侵入された場合、その設備の物理構成やシステム構成が漏洩する可能性が高いため）、情報を保護するための物理セキュリティとしてビル管理システムや監視システムも含まれています。

自社製品に使われている他社製品なども対象となり、さらにその他社製品に使われている製品も対象となるため、対象になる企業は莫大なものとなります。日本の防衛省も防衛調達にこの基準を採用することになり、対象となる企業は9,000社に上ると言われています。米国政府あるいは日本の防衛省と直接取引をしていなくても、サプライチェーンの中に組み込まれている企業は全て対象となるため、知らない間に準拠を求められていたという日本企業も少なくないでしょう。

EUでは2016年7月6日にNIS指令（「The Directive on Security of Network and Information Systems」＜ネットワークと情報システムのセキュリティに関する指令＞）が成立しました。加盟各国に指令に準拠した法令を整備することを求めるもので、既にEU各国は法令の整備を行っています。NIS指令はエネルギー、運輸、医療、水道などの重要インフラ事業者を対象としており、ICS製品やサービス事業者にとって無視できないものとなっています。この法律が定めるセキュリティ基準を満たさない場合、2021年6月28日以降は処罰されることになります。最大2,000万ユーロまたは企業における全世界の売上高の4%を罰金として課されます。

これらは世界各地で進んでいるICSセキュリティ強化の一例に過ぎません。今後、さらにICSセキュリティ向上のための法令や制度が整備されていき、製品やサービスはそれらへの準拠が求められることになることは明白です。

中国やロシアはICSに対する研究に力を注いでおり、世界中のPLC（Programmable Logic Controller）の脆弱性を調査していると言われています。現に、中国を拠点とする研究者によるICSセキュリティに関する論文は年々増加しています。中国とロシアが今後、脆弱性のある製品を購買しなくなる可能性も十分に考えられます。ICSセキュリティへの対応の遅れはこうした国々でのビジネスを妨げる要因になりかねず、さらに言えば、今後の世界経済の中心になる可能性があるアフリカやラテンアメリカ市場を失うことにもつながる危険があるのです。

国家をあげたICSセキュリティ研究が進行中

前述のように、世界各国はICSセキュリティに注力するようになっています。その中でも特にロシアと中国の動きは目覚ましく、世界をリードしていると言っても過言ではありません。ロシアや中国は、重要な課題となっているICSセキュリティの研究に国家をあげて取り組んでおり、ベストプラクティスと呼んでもよいでしょう。

ロシアでは中央科学研究機構（CNIIHM＝the Central Scientific Research Institute of Chemistry and Mechanics）がICSセキュリティに関する研究を行っています。雑誌『MIT Technology Review』で「世界で最も殺人的なマルウェア」と評されたTRITONやAPTへの関与が疑われているほどです（※2）。

中国でも大学や研究機関をもとに構成される国家重点実験室（State Key Laboratory：SKL）をはじめとし、ICSセキュリティの研究が活発化しています。同実験室には「学科国家重点実験室」、「企業国家重点実験室」と「省部共建国家重点実験室」の3つの研究拠点があります。この中で、制御理論やシステム工学などを研究する産業制御技術国家重点実験室のテーマには「ICSセキュリティ」が加えられ、また産業情報技術省重点実験室の研究テーマに「ネットワークセキュリティ」が加えられるなど、セキュリティ研究にシフトしていることが分かります。この動きは、5月に開催された中国両会において、産業用インターネットが今後のキーワードの1つとして挙げられていることから、さらに強化されることが予想されます。

また、SKLでは組織の枠を超えた連携が実現されており、中国のトップレベルの大学の頭脳が結集して研究に当たっています。海外から優秀な研究者を招聘する「千人計画」にも組み込まれていることからも、力の入れ方が伺えます。研究結果の一部は脆弱性報告として当該メーカーへ報告されています。

各国の研究で興味深いのは、中国に関わらず、これらの国営研究機関には、安全保障に関連する組織も関与していることです。ICSが今後の各国の経済成長に影響を与えることは、米国や中国の経済摩擦の状況に鑑みても明らかです。つまり、ICSセキュリティは、自国の経済活動を停止させないためにも重要な要素といえ、これまで以上に対策が求められるようになると予想されます。

ロシアと中国の詳細な研究内容は明らかではありませが、こうした分野の研究を行う以上、レッドチームが必要になることから攻撃手法およびゼロデイ脆弱性の研究を行っている可能性が高いと言えるでしょう。特にICSセキュリティの要の一つであるPLCについては世界中の製品を集めて、研究を行っていると言われています。当然、日本のPLCも対象であると考えられます。

同様の研究はアメリカをはじめとする各国でも行われており、国、民間、研究機関が連携しています。

図表1：PLCをターゲットにした脆弱性、マルウェアの例

名称	ターゲット	
Rogue7	電子機器メーカーのオートメーションシステム	2019,米国,Black Hat発表
URGENT／11	組み込みシステム向けリアルタイムオペレーティングシステム	2019,米国セキュリティベンダーが公開
PLC Blaster	電子機器メーカーのオートメーションシステム	2016,米国,Black Hat発表

大幅に立ち遅れた日本企業

日本においては技術研究組合制御システムセキュリティセンター（CSSC）、経済産業省の産業サイバーセキュリティ研究会、情報処理推進機構（IPA）の産業サイバーセキュリティセンターおよび産業総術研合研究所サイバーフィジカルセキュリティセンター（CPSEC）などをはじめとする各機関が、ICSセキュリティの向上と啓発に努めています。また、経産省が提唱する「Connected Industries」においてもICSセキュリティが重要な課題として挙げられ、国土交通省、厚生労働省などをはじめとする各省庁も真剣に取り組んでいます。

ICSセキュリティは民間企業の課題である以上に安全保障上の問題であり、米国やロシア、中国のように国家が民間と連携して横断的、統合的に取り組む必要があるものです。残念ながら日本の体制はそこまでには達しておらず、省庁や官民学の枠を超えた連携は今後の課題です。

民間企業への啓発も遅れており、脆弱性報告があってもすぐに対応できない、あるいは一部しか対応できないといったことは珍しくありません。インターネット上では、脆弱性のある日本企業の製品が他の日本企業に使われていたり、パスワードをハードコーディングしている製品が存在したりする事実が公にされています。こうした状況は、一刻も早く改善されなければなりません。

中でも、各国で研究が進んでいるPLCを製造する企業は注意が必要です。研究が進んでいるということは、攻撃に悪用されかねない脆弱性が発見される頻度が増えるとともに、その脆弱性を持つ製品が購買や調達から外される可能性をはらんでいるからです。

ICSセキュリティの早急な体制確立のために

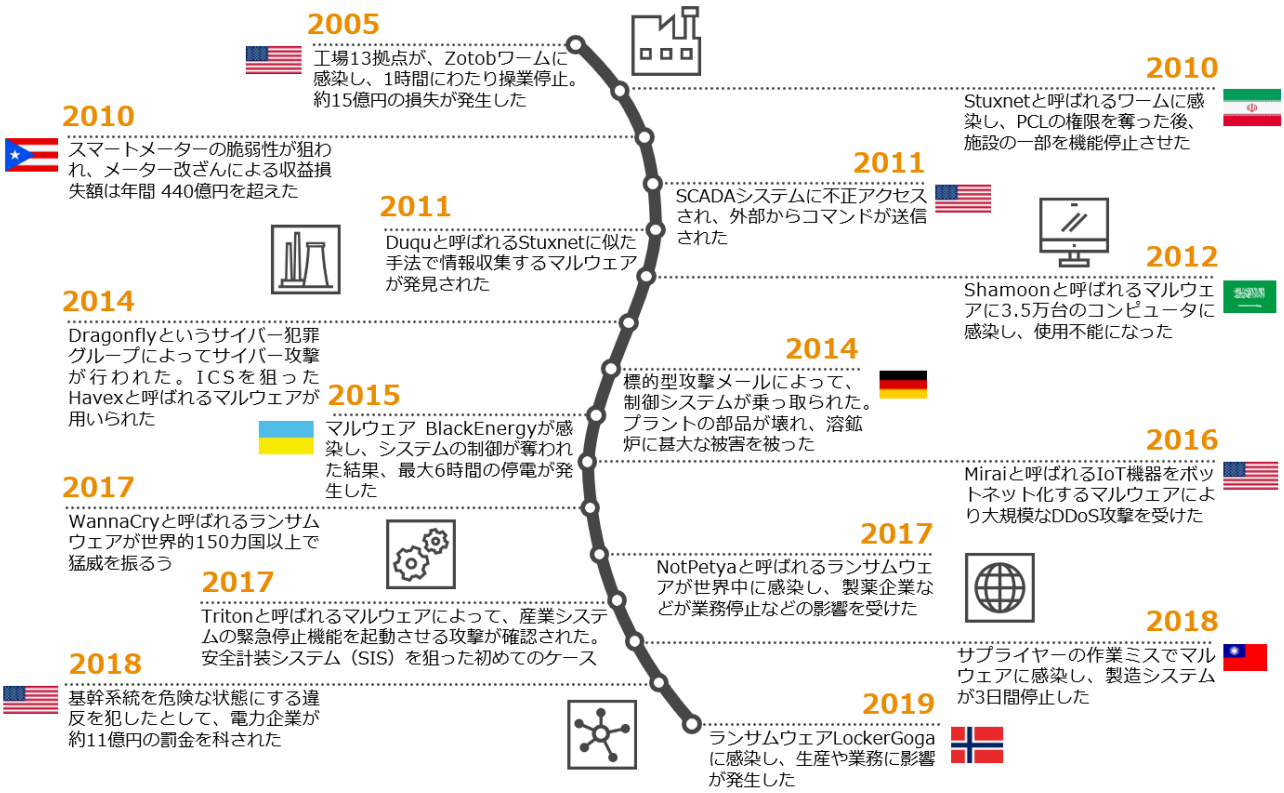
日本政府を中心とした取り組みは行われてはいるものの、目の前の脅威に対抗できる状態には至っていないのが現状と言わざるを得ません。日本全体での有効な枠組みが出来上がるまでは、企業自ら、身を守るための対処をしなければなりません。特に重点的に研究が行われ、攻撃も増加しているPLCのメーカーや利用企業は、早急な体制の確立が必要です。そのためには脅威情報の収集とその適切な活用が重要と考えられます。

ICSセキュリティの脆弱性対応とパッチマネジメントにはITセキュリティとは違う、特有の大きな問題があります。脆弱性もパッチも、必要かつ検証されたものだけを適切なタイミングで迅速に対応しなければならないのです。2019年に行われたセキュリティ企業主催のあるセミナーでは、報告されているICSセキュリティ脆弱性の64%は実際にはリスクを引き起こさず、さらに34%は不正確と指摘されています（※5）。

日本ではICSセキュリティ関係の脆弱性が積極的に報告もしくは公開されていないのが実情です。これにより、報告されている脆弱性だけでは十分な対処を行えない可能性があります。

脅威情報を活用することで、狙われている機器や脆弱性、攻撃方法を事前に察知し、備えることができます。また、攻撃グループの狙いを知ることも防御の上では役に立ちます。ICSセキュリティは、緒に就いたばかりです。各国あるいは攻撃グループが研究している内容が実戦に投入されるこれからが本番と言えるでしょう。

工場・発電所などへのサイバー攻撃



執筆者

名和　利男

PwC Japan グループ
サイバーセキュリティ
最高技術顧問

林　和洋

PwCコンサルティング
合同会社
パートナー

岩井　博樹

PwC Japan グループ
スレットインテリジェンス
アドバイザー

村上　純一

PwCコンサルティング
合同会社
ディレクター

PwC Cyber Security & Privacy

https://www.pwc.com/jp/ja/services/digital-trust.html

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約8,100人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界157カ国に及ぶグローバルネットワークに276,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.com をご覧ください。

© 2020 PwC. All rights reserved. PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.