Ⅱ-3
制御系におけるサイバーセキュリティ

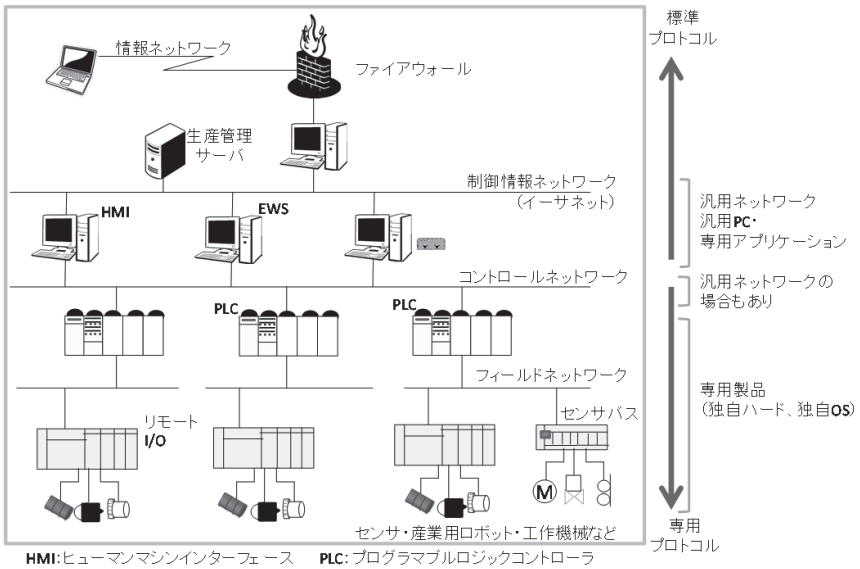
3.1　制御システム

制御システムは、製造業などのほか、発電所や上下水道施設、石油化学プラントなどの重要インフラで監視・制御に利用されている。制御システムのセキュリティインシデントが増加しており、セキュリティ強化のための政策が進められている。

制御システムとは、センサや産業用ロボット、工作機械などの工場・プラントの現場で計測制御に用いられているフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアントPCなどをネットワークで接続したシステムである。自動車や精密機械、食料品、医薬品などの製造業の工場・プラントのほか、電力、ガス、水道、通信、石油化学プラントなど、国民生活及び社会経済活動の基盤となっている重要インフラで監視・制御に使われている。

制御システムは、独立した専用システムとして設計されてきたことから各事業者が独自のシステムや通信プロトコルを採用していた。しかしながら、近年、コスト削減などの経済性や相互接続性の確保、PCやネットワーク技術の高性能化・高度化により、汎用技術・製品の導入が進展している（制御システムの構成例と汎用技術・製品の導入状況を図1に示す）。これに伴い、脆弱性リスクの混入の可能性が指摘されている。同時に、制御システムは通常10～20年にわたって使用されるものであり、導入時のセキュリティ対策技術が陳腐化する点からも、セキュリティ課題が顕在化している。(1) 制御システムにインシデントが発生し、システムの停止や不正操作につながった場合、多大な経済損失や人命に危険が生じる可能性がある。

図1　制御システムの構成例



（出典）情報処理推進機構「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」2009.3, p18. <http://www.ipa.go.jp/files/000013981.pdf>を基に三菱総合研究所作成。

米国で制御システムのインシデントや脆弱性への対応を実施しているICS-CERTの発表によると、実際に米国では制御システムのセキュリティインシデントが2013年には256件報告されている(2)。日本国内においても、JPCERTコーディネーションセンター（JPCERT/CC）がICS-CERTのカウンターパートとして2013年1月から制御システムのインシデント報告の受付を開始

しており(3)、2014年9月には6件の制御システム関連のインシデントの発生を報告している(4)。

●事例研究

■制御システムセキュリティセンター（CSSC）

2012年3月に、制御システムベンダ、セキュリティベンダ、制御システムのユーザ企業、大学、独立行政法人等が参加し、CSSCが発足した。CSSCでは、重要インフラの制御システムのセキュリティ確保を目的として、研究開発、国際標準化活動、評価認証、人材育成、普及啓発、セキュリティ検証を進めており、例えば制御システムの高セキュア化技術の研究開発、模擬プラントを利用した電力・ガス・ビル・化学分野でのサイバーセキュリティ演習、制御システムのセキュリティに関する評価認証であるISASecure EDSA認証などを実施している。(5)

●海外の状況、技術動向、制度、規制

■ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）

ICS-CERTは米国国土安全保障省（Department of Homeland Security: DHS）の下で重要インフラの制御システムのセキュリティを担当する機関として2009年に設立された。制御システムが関連するインシデントへの対応と分析、制御システム製品の脆弱性の分析と取扱の調整、サイバー攻撃を受けた事業者への現地対応を含む改善支援、各種情報の提供等を実施している。(6)

■ENISA（European Union Agency for Network and Information Security）

ENISAは欧州連合（EU）の機関であり、ネットワークセキュリティ及び情報セキュリティに関して、欧州委員会や各加盟国に提言を行っている(7)。制御システムのセキュリティについても提言を行っており、2011年には制御システムの防護に関する報告書を発表している(8)。

■ENCS（European Network for Cyber Security）

ENCSは欧州の重要インフラのセキュリティを高めることを目的としたNPOであり、重要インフラに関連した研究開発や試験、教育・トレーニング、情報共有などの活動を行っている(9)。2013年12月にはCSSCと協力覚書を締結した(10)。

---

(1)　情報処理推進機構「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」2009.3, p21. <http://www.ipa.go.jp/files/000013981.pdf>

(2)　Industrial Control Systems Cyber Emergency Response Team,“ICS-CERT Year in Review 2013,”February 24, 2014, p.16. <https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf>

(3)　JPCERTコーディネーションセンター「JPCERT/CC 活動概要（2013年1月1日～2013年3月31日）」2013.4.15, p.1. <https://www.jpcert.or.jp/pr/2013/PR20130415.pdf>

(4)　JPCERTコーディネーションセンター「JPCERT/CCインシデント報告対応レポート（2014年7月1日～2014年9月30日）」2014.10.9, p.3. <https://www.jpcert.or.jp/pr/2014/IR_Report20141009.pdf>

(5)　制御システムセキュリティセンター「制御システムセキュリティの脅威と対策の動向およびCSSCの研究概要について（一般向け）」2015.2.2, pp.10-23. <http://www.css-center.or.jp/pdf/about_CSSC.pdf>

(6)　“About the Industrial Control Systems Cyber Emergency Response Team.”Industrial Control Systems Cyber Emergency Response Team Website <https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team>

(7)　“About ENISA.”European Union Agency for Network and Information Security Website <https://www.enisa.europa.eu/about-enisa>

(8)　European Network and Information Security Agency,“Protecting Industrial Control Systems: Recommendations for Europe and Member States,”December 9, 2011. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport>

(9)　“About ENCS.”European Network for Cyber Security Website <http://www.encs.eu/about-encs>

(10)　制御システムセキュリティセンター「CSSC、欧州の重要インフラのサイバーセキュリティ推進組織ENCSと協力覚書を締結―グローバルな連携で重要インフラのセキュリティ向上を目指す―」2013.12.2. <http://www.css-center.or.jp/ja/info/documents/press/press_20131202.pdf>

3.2　制御システムセキュリティに関する国際標準・認証

制御システムセキュリティに関する様々な業界標準が存在する中、一部の業界標準を国際標準IEC 62443に統合する動きが進展している。一方、日本では、2014年にISA Secure EDSA認証及びCSMS認証業務を開始するなど体制整備が進んでいる。

制御システムのセキュリティの標準・基準には、組織やシステム、機器を対象としたもの、特定の業種や業界を対象としたものなど、様々な標準・基準が提案されており、制御システムの安全性を確保するための基準として活用されている。

業界標準としては、WIB（International Instrument Users' Association）[(1)]による基準や北米電力信頼度協議会（North American Electric Reliability Corporation: NERC）によるNERC CIP（Critical Infrastructure Protection）[(2)]が挙げられる。WIBは、ロイヤル・ダッチ・シェルやBP（British Petroleum）などの大手石油企業が加入する業界団体であり、石油・化学プラントを対象とした基準を策定している。NERC CIPはNERCによる北米の電力事業者向けの発電と送電に関わるセキュリティ基準である。

現在、多くの制御システムセキュリティに関する業界標準が存在する中で、汎用的な標準・基準として、国際標準のIEC62443の策定が進められている。評価認証スキームで既に先行しているISCI（ISA Security Compliance Institute）[(3)]やWIBの基準を、IEC 62443シリーズに統合する動きが進展しており、一部事業者の調達要件にもなってきている[(4)]。

一方、認証の枠組みとしては、ISCIにおいて、制御システムセキュリティに関する評価認証プログラムISA Secure Certificationsの開発が進められており[(5)]、ほかにもカナダのWurldtech社によるAchilles認証などが整備されている[(6)]。

セキュリティに関する国際認証を迅速に取得することは、制御システムの安全性の確保という点に加えて、制御機器・システムベンダの国際競争力強化という観点でも重要である。そこで、経済産業省及び情報処理推進機構（IPA）は、認証を国内で取得可能とし、認証取得を容易化するため、国内での認証制度確立のための取組を2012年度から推進してきた。

制御装置を対象としたセキュリティ保証に関する認証制度であるISA Secure 組込みデバイスセキュリティ保証（Embedded Device Security Assurance: EDSA）認証は当初、ISCIのほか、認定機関をANSI（American National Standards Institute）、評価及び認証機関を米国exida社が担うなど、全て北米の組織で構成されており、日本国内からのEDSA認証取得は手続面で難しさがあった。それに対して、日本では、IPAが2012年9月にISCIと相互協力の関係を結び、規格書の対訳版を公開するなど、認証制度の確立・普及に向けた取組を進めてきた[(7)]。2013年には、経済産業省の支援のもと官民学が連携し2012年3月に設立された制御システムセキュリティセンター（CSSC）がパイロット認証プロジェクトを実施し、2014年4月から世界で2番目のEDSA認証機関として正式に評価認証業務を開始している[(8)]。

また、情報セキュリティマネジメントシステム（ISMS）の制御システム版に相当する制御システムに関するセキュリティマネジメントシステム（Cyber Security Management System for IACS (Industrial Automation and Control System): CSMS）の認証も推進されている。CSMS認証はIEC62443-2-1を基準とした認証制度であり、制御システムの製造やオペレーションを行う企業がセキュ

リティに関して取り組むべき組織マネジメントについて国際標準に適合していることを認証するものである。日本ではCSMS認証体制を世界に先駆けて確立しており、日本情報経済社会推進協会（Japan Institute for Promotion of Digital Economy and Community: JIPDEC）の認定のもと、民間事業者である日本品質保証機構とBSIグループジャパンが認証機関となり、2014年4月、三菱化学エンジニアリングと横河ソリューションサービスが世界で初めて認証を取得した。(9)

●海外の状況、技術動向、制度、規制

■北米の電力セクター向けのセキュリティに関する規格・ガイドライン

北米の電力セクター向けのセキュリティ規格・ガイドラインとして、NERC CIPとNISTIR 7628がある。

北米の電力事業者向けのセキュリティ基準であるNERC CIPでは、システムの重要度別にセキュリティ要件とその確認方法が規定されている(10)。NERC CIPは強制力がある基準であり、電力事業者は遵守状況について米国連邦エネルギー規制委員会（FERC）に提出し(11)、NERC CIPが要求する対策要件に違反する場合は罰金が科せられる(12)。

米国国立標準技術研究所（National Institute of Standards and Technology: NIST）が2010年9月に発表したNISTIR 7628は、スマートグリッドのセキュリティについて示したガイドラインである。NISTIR 7628はスマートグリッドのセキュリティ要件の定義や、スマートグリッドに接続される一般家庭のプライバシー問題などを扱っている。(13)

---

(1)　International Instrument Users' Association WIB Website <http://www.wib.nl/>
(2)　“CIP Standards.”North American Electric Reliability Corporation Website <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>
(3)　2007年に米国を中心として設立された、制御システムに係る規格の標準化活動及び普及啓発活動等を実施する国際的なセキュリティ認証推進組織。
(4)　制御システムセキュリティセンター「制御システムセキュリティの脅威と対策の動向およびCSSCの研究概要について（一般向け）」2015.2.2, p.19. <http://www.css-center.or.jp/pdf/about_CSSC.pdf>
(5)　“ISA Secure® Certifications.”ISA Security Compliance Institute Website <http://www.isasecure.org/en-US/Certification>
(6)　“Wurldtech Certification Programs.”Wurldtech Security Technologies Inc. Website <http://www.wurldtech.com/product_services/certifications/>
(7)　情報処理推進機構「制御機器認証プログラム「EDSA」国内認証制度の確立および規格書対訳版の公開について―認証制度の確立・普及に向けたパイロットプロジェクトの推進―」2013.4.15. <https://www.ipa.go.jp/files/000026491.pdf>
(8)　制御システムセキュリティセンター「制御システムセキュリティセンター、セキュア制御機器の製品認証を開始―制御システム用機器の輸出力向上を目指し、アジアでの最初のEDSA認証機関となる―」2014.3.31. <http://www.css-center.or.jp/ja/info/documents/press/press_20140331.pdf>
(9)　「世界初！制御システムのセキュリティマネジメントシステム（CSMS）の国際標準に対する認証を日本企業が取得しました」2014.4.25. 経済産業省ウェブサイト <http://www.meti.go.jp/press/2014/04/20140425003/20140425003.html>
(10)　前掲注(2)
(11)　“CIP Compliance.”North American Electric Reliability Corporation Website <http://www.nerc.com/pa/CI/Comp/Pages/default.aspx>
(12)　“Compliance & Enforcement.”North American Electric Reliability Corporation Website <http://www.nerc.com/pa/comp/Pages/Default.aspx>
(13)　The Smart Grid Interoperability Panel Cyber Security Working Group,“Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security,”September 2010. National Institute of Standards and Technology Website <http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf>

3.3　組込みシステム

組込みシステムとは、産業機器や家電製品などの機器に組み込まれ、機器の制御を行う目的に専用化されたコンピュータシステムである。組込みシステムのセキュリティについて、ガイド作成や普及啓発が情報処理推進機構等により実施されている。

組込みシステムとは、半導体やその周辺装置からなる部分で、機器の制御を行う目的に専用化されたコンピュータシステムであり、産業機器や家電製品、自動車などの機器に組み込まれ、様々な分野で利用されている。日本標準産業分類（平成26年4月施行）では組込みソフトウェア業（3912）として位置付けられている。組込みシステムの主要関連産業である製造業はGDPの18.0%（2012年）を占めるなど(1)、組込みシステムは我が国の産業の基盤を支えている。

組込みシステムは、情報通信技術の進展により、インターネットなどのオープンなネットワークに接続されるようになりつつあり、パソコンと同様に、ネットワークを介した第三者による攻撃の脅威にさらされる可能性が高まっている(2)。情報処理推進機構（IPA）の報告書によると、携帯電話やスマートフォンに特化したOSである「Symbian OS」を搭載した携帯電話に感染するウイルスが海外で多数発見された事例や、北米でATM、POS端末等の専用システムが感染しサービス不能に陥った事例などがある(3)。

このような状況に対して、IPAでは2006年から組込みシステム全般のセキュリティ調査や、組込み機器のセキュリティガイドの作成、組込み機器のセキュリティに関する普及啓発を実施している。2009年には、組込みシステムの開発関係者を対象とした「組込みシステムのセキュリティへの取組みガイド」(4)を作成・公開し、①開発チームのマネジメント面、②組込みシステムの企画・開発面、③組込みシステムの利用時において開発元が行うべき運用面、④組込みシステムの廃棄面に関して行うべき取組事項を、セキュリティへの取組のレベルごとに提示している。

また、組込みシステムが利用されている情報家電(5)や自動車、医療機器についても、IPAにおいて、セキュリティ上の課題や対策の検討が実施されている。情報家電については、家電業界各社と経済産業省が参加して、2010年3月から同年12月に勉強会を実施し、2011年2月、「2010年度版 情報家電におけるセキュリティ対策 検討報告書」(6)を公開している。自動車に関しても、2013年3月、自動車本体や車載機器の企画段階から廃棄段階に至る検討すべき情報セキュリティ上のポイントをまとめた「自動車の情報セキュリティへの取組みガイド」(7)と、国内外における自動車セキュリティ関連情報を調査した「2012年度 自動車の情報セキュリティ動向に関する調査報告書」(8)を公開している。組込みソフトウェアに関する保有スキルや求められるスキルを可視化する「組込みスキル標準（ETSS）」(9)、組込みソフトウェアの開発を円滑に進めるための標準的な作業やベストプラクティスを示した「組込みソフトウェア向け開発プロセスガイド」(10)など、組込みソフトウェア分野の人材育成や組込みソフトウェアの高信頼化に関する取組も行われている。

ほかにも、2006年に制定された「中小企業のものづくり基盤技術の高度化に関する法律」（いわゆる「中小ものづくり高度化法」。平成18年法律第33号）に基づき、経済産業省により、組込みソフトウェアに関する研究開発に対し支援などが行われている(11)。

●事例研究

■POSシステムを標的としたサイバー攻撃

米国ではPOSシステムを狙うマルウェアによる攻撃が増加している。マルウェアはPOSシステムに感染し、クレジットカード情報などを収集するとされている。米国では2014年第1四半期だけで、大手企業のPOSシステムのハッキングが4件発覚しており、2013年12月には1億1千万件のクレジットカード・デビットカードの情報漏えいが発覚している。(12)

2014年6月には、日本においてもPOSシステムのマルウェア感染が確認されたと報道されている(13)。

●海外の状況、技術動向、制度、規制

■欧州の自動車セキュリティに関する検討状況

欧州では、自動車のセキュリティの先駆けとされるEVITA（E-safety vehicle intrusion protected applications）プロジェクトがEUの支援で2008年から2011年にかけて行われ、自動車におけるセキュリティ課題の整理やセキュリティ機能を搭載したデバイスの開発が進められた(14)。2011年1月には、EVITA等で開発・検討した自動車に関するセキュリティ技術の量産化・低価格化を目的としたPRESERVE（Preparing Secure Vehicle-to-X Communication Systems）プロジェクトも開始されている(15)。

---

(1)　内閣府「2012年度国民経済計算（2005年基準・93SNA）」2013.12. <http://www.esri.cao.go.jp/jp/sna/data/data_list/kakuhou/files/h24/tables/24fcm3n_jp.xls>
(2)　情報処理推進機構「組込みシステムのセキュリティへの取組みガイド（2010年度改訂版）」2010.9, p.3. <http://www.ipa.go.jp/files/000014117.pdf>
(3)　情報処理推進機構「組込みソフトウェアを用いた機器におけるセキュリティ別紙2」2006.4, pp.8-9. <http://www.ipa.go.jp/files/000013783.pdf>
(4)　情報処理推進機構「組込みシステムのセキュリティへの取組みガイド」2009.6. <https://www.ipa.go.jp/files/000013968.pdf>
(5)　情報家電とは、「携帯電話、携帯情報端末（PDA）、テレビ、自動車等生活の様々なシーンにおいて活用される情報通信機器及び家庭電化製品等であって、それらがネットワークや相互に接続されたものを広く指す。」と定義されている。情報家電の市場化戦略に関する研究会「基本戦略報告書「e-Lifeイニシアティブ」」2003.4, p.4. 国立国会図書館インターネット資料収集保存事業ウェブサイト <http://warp.da.ndl.go.jp/info:ndljp/pid/285403/www.meti.go.jp/kohosys/press/0003917/0/030411e-life.pdf>
(6)　情報処理推進機構「2010年度版情報家電におけるセキュリティ対策検討報告書」2011.1. <http://www.ipa.go.jp/files/000014114.pdf>
(7)　情報処理推進機構「自動車の情報セキュリティへの取組みガイド」2013.3. <http://www.ipa.go.jp/files/000027273.pdf>
(8)　情報処理推進機構「2012年度自動車の情報セキュリティ動向に関する調査報告書」2013.3. <http://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_report_24.pdf>
(9)　「組込みスキル標準（ETSS Series）」情報処理推進機構ウェブサイト <http://www.ipa.go.jp/sec/softwareengineering/std/etss.html>
(10)　情報処理推進機構ソフトウェア・エンジニアリング・センター編『組込みソフトウェア向け開発プロセスガイド: ESPR Ver.2.0』翔泳社, 2007. <http://www.ipa.go.jp/sec/publish/tn07-005.html>
(11)　経済産業省「中小ものづくり高度化法の概要」2012, p.1. <http://www.meti.go.jp/committee/chuki/keieishien/gijutsu/001_02_00.pdf>
(12)　トレンドマイクロ「TrendLabs 2014年第1四半期セキュリティラウンドアップ 新たな獲物を見つけたサイバー犯罪者―狙われたPOSシステムと仮想通貨―」2014.5.20, p.39. <http://www.trendmicro.co.jp/cloud-content/jp/pdfs/security-intelligence/threat-report/pdf-2014q1-20140520.pdf?cm_sp=Corp-_-sr-_-2014Q1>
(13)「POS：ウイルスまん延　レジと一体、カード情報危険に　国内で検出数急増、感染も」『毎日新聞』2014.6.30, 夕刊.
(14)　“Work plan,”2011.4.15. E-safety vehicle intrusion protected applications Website <http://www.evita-project.org/work_plan.html>
(15)　“About the Project.”PRESERVE project Website <http://www.preserve-project.eu/about>

主要事項執筆者一覧

執筆者所属：三菱総合研究所

執筆者	主要事項
情報通信政策研究本部主席研究員　村野（むらの）　正泰（まさやす）	1.3.1, 4.1, 4.2, 4.3, 4.4, 4.6, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.1, 5.3.2, 6.2.1
情報通信政策研究本部主席研究員　澤部（さわべ）　直太（なおた）	1.3.2, 1.3.3, 1.3.4
情報通信政策研究本部主任研究員　谷田部（やたべ）　智之（ともゆき）	1.1, 1.2.1, 1.2.3, 1.2.4, 1.3.6, 2.4, 6.2.6, 6.2.7
情報通信政策研究本部主任研究員　清水（しみず）　友晴（ともはる）	6.1.1
情報通信政策研究本部研究員　松本（まつもと）　尭（たかし）	1.2.5, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 4.5
情報通信政策研究本部研究員　丸田（まるた）　佳織（かおり）	1.2.2, 1.3.5, 5.1.4, 5.2.5, 5.2.6, 6.1.2, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 7.1, 7.2, 7.3

＊ 本稿におけるインターネット情報の最終アクセス日は、原則として、2015年1月13日である。