制御系におけるサイバーセキュリティ

要　旨

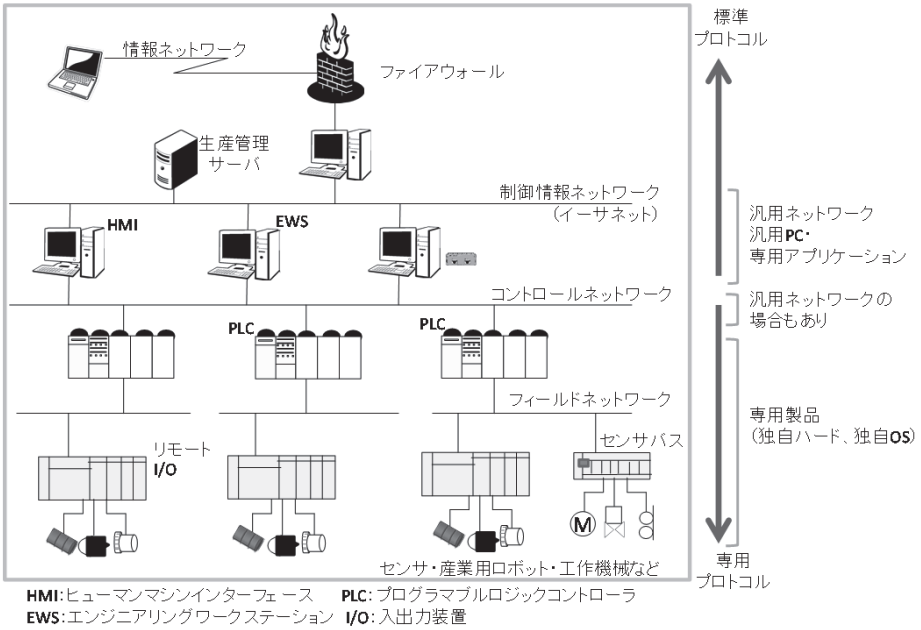
制御システムは、製造業の工場・プラントのほか、発電所や上下水道施設などの社会インフラで利用されているシステムであり、組込みシステムは自動車や家電製品などの機器に組み込まれているシステムである。これらのシステムは、社会インフラを支えるものから日常生活で消費者が利用しているものまで多分野にわたり、社会経済にも影響が大きいものである。機器のオープン化等に伴い、近年、これらのシステムに対するセキュリティリスクが顕在化し始めている。同時に、スマートメーターやネットワークにつながる自動車など、新たなシステムに対しても同様の脅威が指摘されている。そこで、セキュリティ検討組織の立ち上げやガイドの策定など、セキュリティの検討及び強化が進められつつある。

I　制御システムのセキュリティ

1　オープン化・ネットワーク化によるリスクの顕在化

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。具体的には、制御システムにより、ゲートの開閉や薬品などのバルブの開閉、モータの起動停止などの制御が行われ、その状態が監視されている。

図1　制御システムの構成例



HMI:ヒューマンマシンインターフェース　PLC:プログラマブルロジックコントローラ
EWS:エンジニアリングワークステーション　I/O:入出力装置

（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, p.18. <http://www.ipa.go.jp/files/000013981.pdf>を基に三菱総合研究所作成。

＊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。

制御システムは、図1に示すように、一般的に階層構造となっており、制御情報ネットワーク、コントロールネットワーク、フィールドネットワーク等で構成される。フィールドネットワーク等の産業プラントや工場の現場で利用されるネットワークを産業用ネットワークといい、フィールドネットワークには制御対象であるセンサや産業用ロボット、工作機械などの機器と、それらの機器をリアルタイムに制御するPLC（Programmable Logic Controller）等のコントローラが接続されている。さらに、PLCや監視・操作のためのHMI（Human Machine Interface）が接続されているコントロールネットワークがあり、それらより上位に生産管理サーバ等が接続されている構成となっている。これらの制御システムは現在では、一般にファイアウォールを介して外部の情報システムと接続している。(1)

近年、これらの制御システムに関して、セキュリティ課題が顕在化してきている。その要因としては、汎用製品の利用や標準のプロトコルの採用などのシステムのオープン化と、外部のネットワークに接続するネットワーク化が挙げられる。

従来、制御システムで利用されている機器及びプロトコルはベンダ独自のものが用いられてきた。しかしながら、コスト削減などの経済性やPCの高機能化などにより、HMIやEWS（Engineering Work Station）に採用される端末はWindows等が搭載された汎用PCが主流となっており、制御情報ネットワークや一部のコントロールネットワークではイーサネットやTCP/IPなど情報システムで一般的なプロトコルが採用されている。こういった汎用製品・プロトコルの採用により、これらの汎用製品における脆弱性の課題も引き継ぐこととなり、たとえファイアウォールが設置されていてもセキュリティリスクが生じている。

さらに、ネットワーク技術の高度化に伴い、生産管理の効率化による競争力強化等を目的として制御システムとオフィスの情報システム等をシームレスに接続するケースが常態化しつつある。制御システムをほかの情報システムや外部ネットワークと接続するネットワーク化により、ウイルスの侵入や機密情報漏えいのリスクが増大している。

これらの要因に加えて、重要インフラ系の制御システム特有の事情として、システムが継続して稼働することが重視されるために脆弱性対策のパッチ適用が困難なことや、システム負荷の観点からウイルスチェックの実施が困難なこと、製品を通常10～20年の長期にわたって利用し続けるためセキュリティ対策技術が陳腐化することなどもある。さらに、標的型のマルウェアによる特定の制御システムを狙ったサイバー攻撃が発生するなど脅威も増大している。制御システム側の要因に加えて、サイバー攻撃の脅威の増大といった外的要因もあり、制御システムのセキュリティ課題が急速に顕在化しつつある。

2　セキュリティインシデントの現況

制御システムへのサイバー攻撃として大きなインパクトを与えたのが、2010年のイランのウラン濃縮施設へのサイバー攻撃で発見されたStuxnet（「スタックスネット」と読む。）(2)である。

(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, pp.18-19. <http://www.ipa.go.jp/files/000013981.pdf>

(2)　JPCERTコーディネーションセンター「Stuxnet―制御システムを狙った初のマルウェア―」2011.2, pp.3-24. <https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf>

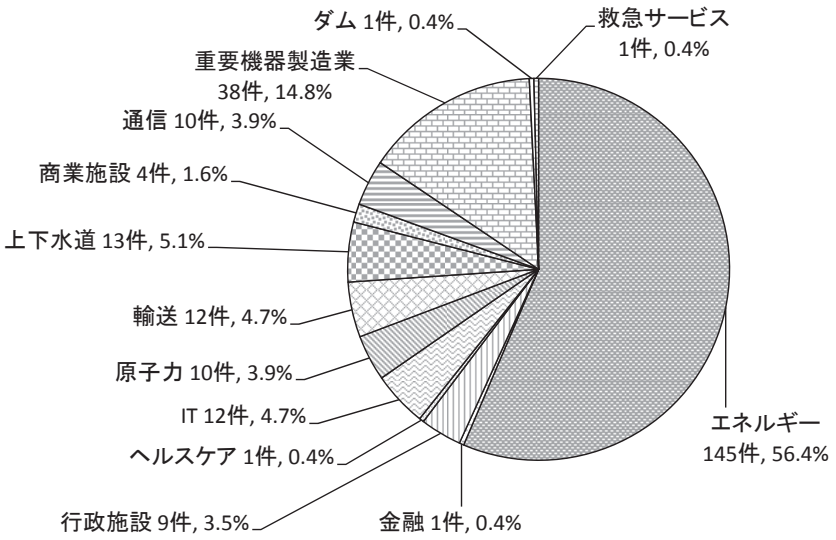
Stuxnet以前にも制御システムにおけるインシデントは発生していたものの、Stuxnetは制御システムを標的とした初のマルウェアとされ、同施設の約8,400台の遠心分離機を全て停止させるなどの被害を引き起こした(3)。Stuxnetは特定の制御システムのみで動作するよう作られたマルウェアであり、技術面でも非常に複雑で巧妙な構造となっている。そのため、国家の関与が疑われており、2012年にはニューヨークタイムズ紙が米国国家安全保障局（National Security Agency: NSA）とイスラエル軍の情報機関がStuxnetを作成したと報じた(4)。

Stuxnet以前にも重大なインシデントは発生している。2000年にはオーストラリアにおいて、SCADA（Supervisory Control and Data Acquisition）ソフトウェア(5)の開発企業の元従業員が、下水処理の制御システムに侵入し、下水排水施設のデータを書換えるなどのオペレーションの妨害を行い、その結果、約27万ガロン（約1,022kL）の未処理下水を河川や公園に放出する事態となった(6)。また、2003年には米国の原子力発電所の制御システムが情報システムを標的としたSlammerワームに感染し、5時間にわたって停止する事態となっている(7)。2014年にはStuxnet以来とされる制御システムを標的としたマルウェアHavexが発見され、欧州、米国を中心に感染が報告されている(8)。セキュリティインシデントは日本でも起こっており、自動車メーカーや半導体メーカーの工場の生産ラインが停止するなどの事態に陥ったケースもある(9)。

米国ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）(10)は、制御システムが関連するインシデントへの対応と分析を実施しており、米国2013会計年度には257件のインシデントがあったと報告している。米国2011会計年度140件、米国2012会計年度197件と近年急激に増加しており、分野別に見るとエネルギー分野のインシデント145件（米国2013会計年度）が最も多く、続いて重要機器製造業、上下水道の順となっている（図2参照）。(11)

(3)　同上
(4)　“Obama Order Speed Up Wave of Cyberattacks Against Iran,” *The New York Times*, June 1, 2012. <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>
(5)　SCADAソフトウェアとは、制御機器の監視制御を行うためのソフトウェアのこと。
(6)　TNO Defence, Security and Safety, “SCADA Security Good Practices for the Drinking Water Sector,” March 2008, p.14. <http://www.cpni.nl/files/3813/0388/2940/Scada_security_good_practices_for_the_drinking_water_sector.pdf>
(7)　Kevin Poulsen, “Slammer worm crashed Ohio nuke plant network,” August 19, 2003. SecurityFocus Website <http://www.securityfocus.com/news/6767>
(8)　「産業制御システムを標的とする「HAVEX」とは」（セキュリティ情報）トレンドマイクロウェブサイト <http://about-threats.trendmicro.com/relatedthreats.aspx?language=jp&name=HAVEX%20Targets%20Industrial%20Control%20Systems>
(9)　「サイバー攻撃で工場停止　標的型、制御システム突く　米で被害　社内に潜む侵入口」『日経産業新聞』2012.1.25.
(10)　米国国土安全保障省（Department of Homeland Security: DHS）の下で重要インフラに含まれる制御システムセキュリティを担当する機関。
(11)　Industrial Control Systems Cyber Emergency Response Team, “ICS-CERT Year in Review 2013,” 2014.2.24, pp.14,16. <https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf>

図2　米国ICS-CERTにおけるインシデント件数と分野（米国2013会計年度）



（出典）Industrial Control Systems Cyber Emergency Response Team,“ICS-CERT Year in Review 2013,”2014.2.24, p.14. <https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf>を基に三菱総合研究所作成。

3　政府の取組・課題

制御システムのセキュリティ課題の顕在化に対して、国内では、経済産業省の下、制御システムセキュリティ検討タスクフォースが2011年10月に立ち上げられ、その検討結果を受けて、2012年3月には制御システムセキュリティセンター（CSSC）が発足している。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、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、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証を進めている。具体的には、制御システムのセキュリティを高める技術の研究開発（ホワイトリスト技術(12)の適用、サイバー攻撃の早期認識技術の開発等）、防御技術研究開発のための産業別の9つの模擬プラント構築、その模擬プラントの一部を用いた電力・ガス・ビル・化学分野でのサイバーセキュリティ演習の実施、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（用語集参照）の推進などを実施している(13)。また、CSSCは国際連携も進めており、欧州の重要インフラのレジリエンスを高めることをミッションとするメンバーで構成される非営利の組織ENCS（European Network for Cyber Security）や、スペイン語圏及びポルトガル語圏の制御システムのサイバーセキュリティの普及・啓発推進をミッションとする非営利の組織CCI（Centro de Ciberseguridad Industrial）と相互協力について覚書を締結している(14)。

(12) 端末やサーバにおいてホワイトリスト（通信や実行などの動作を許可する方式又は許可する対象を登録したリスト）によりアプリケーションやプロセスの制御を行う技術や、ファイアウォールやスイッチ等の通信機器においてホワイトリストにより通信の制御を行う技術。

(13) 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>

(14) 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>; 制御システムセキュリティセンター「CSSC、サイバーセキュリティの普及・啓発推進組織CCIと協力覚書を締結―スペイン語圏及びポルトガル語圏への制御システム輸出拡大を目指す―」2014.5.20. <http://www.css-center.or.jp/ja/info/documents/press/press_20140520.pdf>

JPCERTコーディネーションセンター（JPCERT/CC）は、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するなど、制御システム関連のインシデント対応及び情報収集分析活動を実施しており、ICS-CERT等の制御システムに関する海外関係機関との調整活動も担っている(15)。また、制御システムのセキュリティ対策状況を把握するチェックリストと解説書である制御システムセキュリティ自己評価ツール（Check List for Industrial Control Systems of Japan: J-CLICS）を発表するなど、対策の促進に資する活動も進めている(16)。

海外では、2009年に制御システムセキュリティを担当する機関として米国ICS-CERTが設立されている(17)。米国では、2003年の「国土安全保障に関する大統領指令7号」（Homeland Security Presidential Directive 7: HSPD-7）に基づき、2004年に「制御システムセキュリティプログラム」（Control Systems Security Program: CSSP）が米国国土安全保障省（Department of Homeland Security: DHS）で開始されており、ICS-CERTはそのプログラムの一つである(18)。なお、ICS-CERTに対応する国内の機関はJPCERT/CCである。

4　今後の展望

ICS-CERTの報告では前述のように制御システムのインシデントは増加を続けており、2014年にはStuxnet以来となる制御システムを標的としたマルウェアHavexも発見されている(19)。これらの脅威の高まりの一方で、制御システムの現場ではセキュリティ対策が進んでいないことが多い。これは可用性や生産性を重視する制御システム特有の事情や、まだ大多数の企業では制御システムへの脅威を認識していないことが原因となっており、一層の人材育成やユーザ企業への普及啓発が望まれている。

また、導入が進むスマートシティ(20)やスマートメーター（用語集参照）等の新しいシステムに対しても同様のセキュリティ課題が存在する。例えば、東京電力の計画によれば、2014年度から2020年度までの7年間でサービス区域内の全ての世帯にスマートメーターを設置し、ネットワーク経由で家庭や企業の電力消費量を収集、制御するだけでなく、宅内向け通信機能を搭載し、家電などとも連携したサービスを提供していくとされている(21)。こういった高機能なスマートメーターに対し、セキュリティベンダなどから測定の改ざんや電力使用情報の犯罪への悪用、スマートメーターを含めた次世代送電網（スマートグリッド）への攻撃のリスクなどが指摘されている(22)。

---

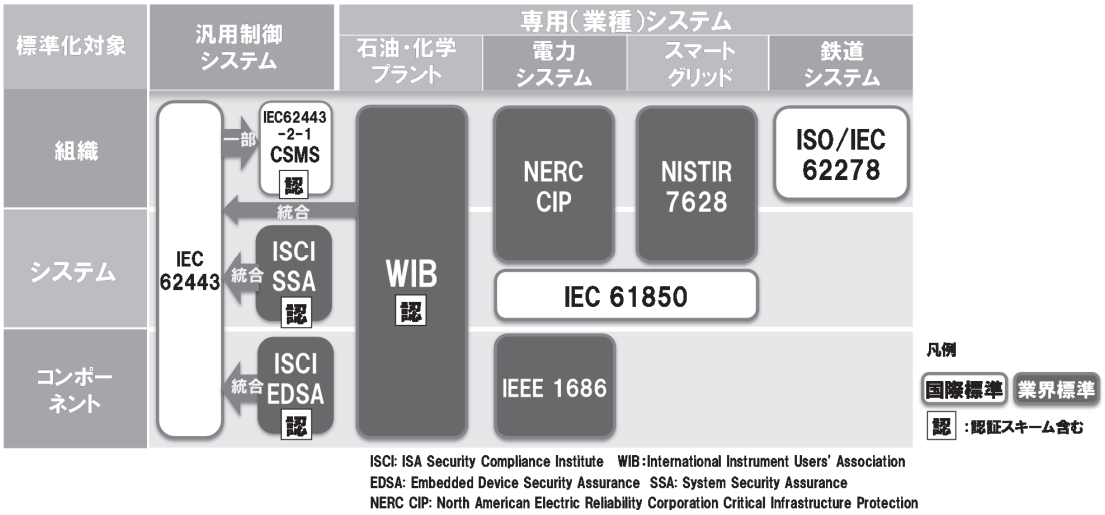
(15) JPCERTコーディネーションセンター「ICS向けJPCERT/CC提供サービスのご紹介」2013.1.24, p.3. <https://www.jpcert.or.jp/ics/2013/ICS20130124-ICSR.pdf>
(16)「制御システムセキュリティ自己評価ツール（J-CLICS）」2013.3.28. JPCERTコーディネーションセンターウェブサイト <https://www.jpcert.or.jp/ics/jclics.html>
(17)“About the Industrial Control Systems Cyber Emergency Response Team.”Industrial Control Systems Cyber Emergency Response Team Website <https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team>
(18) Department of Homeland Security,“Control Systems Security Program.”<http://www.ncfpd.umn.edu/default/assets/File/SlickSheet_CSSP_012411.pdf>
(19) 前掲注(8)
(20) ICTや環境技術などの先端技術を活用することによる市民生活の利便性・快適性の向上や持続可能性の追求、資源の有効活用等を図る都市や地域又はその社会システム。
(21)「スマートメーターについて」東京電力ウェブサイト <http://www.tepco.co.jp/smartmeter/index-j.html>
(22)「すべてをつなぐインターネット（IoE）：スマートメーター、攻撃のシナリオ」トレンドマイクロウェブサイト <http://blog.trendmicro.co.jp/archives/9489>

Ⅱ　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、図3に示すように様々な標準・基準が提案されており、制御システムの安全性の確保のために活用されている。また、一部では認証スキームも整備されている。

これらの標準のうち、認証スキームですでに先行している国際認証推進組織ISCI（ISA Security Compliance Institute）や制御システムのユーザ団体WIB[23]（International Instrument Users' Association）の基準が、制御システムセキュリティに関する国際規格であるIEC 62443のシリーズに統合される動きとなっており、IEC 62443が汎用的な標準・基準として策定が進められている[24]。

図3　制御システムセキュリティに関する標準・基準



（出典）小林偉昭「IEC62443の概要と認証について」2013.11.20, p.17. <http://www.css-center.or.jp/ja/info/documents/2013/20131120_ET2013.pdf>等を基に三菱総合研究所作成。

国内でもIEC 62443に関連した取組が進められている。IEC 62443-4に提案されている制御装置を対象としたISAsecure EDSA（Embedded Device Security Assurance）認証のパイロットプロジェクトが制御システムセキュリティセンター（CSSC）において2013年に実施され、CSSCは2014年4月からISCIのISASecure EDSA認証機関として評価認証業務を開始している[25]。また、日本情報経済社会推進協会（JIPDEC）はIEC 62443-2-1を基準とした認証制度であ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: CSMS）認証のパイロット認証事業を2013年に実施し、2014年4月にはCSMS認証体制が世界に先駆けて日本で確立されている[26]。

(23) Working-party on Instrument Behaviourの略称。1982年以降はInternational Instrument Users' Associationと呼称。
(24) 制御システムセキュリティセンター　前掲注(13), p.19.
(25)「ISASecure® EDSA認証としてのCSSC認証ラボラトリー」CSSC認証ラボラトリーウェブサイト <http://www.cssc-cl.org/jp/aboutus/index.html>
(26)「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>

セキュリティに関する国際認証を取得することは、国際競争力強化やセキュリティ対策の強化の観点で重要であり、前述のように国内での認証制度の確立・普及に向けて取組が進められている。海外ユーザに対して、ベンダが製品を輸出する際、国際標準への準拠及び世界で認められた認証が求められるケースが増加しており、認証取得は国際競争力強化につながる。また、ISMSの制御システム版と対応付けられるCSMS認証のような組織の管理体制（マネジメントシステム）に関する認証を取得すれば、セキュリティ能力の強化に加えて、第三者の視点からセキュリティチェックが可能になり、また組織のブランド力強化につながるなどの利点がある。

III　組込みシステムのセキュリティ

1　組込みシステムのセキュリティに対する取組

組込みシステムとは、機器に組み込まれた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る。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。これらの組込みシステムは、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ることによって、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(27)。このような状況に対して、情報処理推進機構（IPA）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などを実施している(28)。

2　自動車や医療機器における新たな脅威

近年、新たな脅威が顕在化しつつある組込み機器として、自動車と医療機器が挙げられる。自動車では、自動車に組み込まれる電気・電子システムの機能安全の規格であるISO 26262への対応など、安全性についての取組が従来から行われてきたが、近年では、安全性に加えてセキュリティの問題が指摘されている。スマートフォンとの連携や路車間・車車間通信(29)等の新しいネットワークの利用、外部情報を利用したサービスの増加等、自動車を取り巻く環境が変化しており、それに伴うサイバー攻撃による不正操作など、セキュリティ上のリスクが増加している。そのような状況に対し国内では、自動車本体や車載機器の企画段階から廃棄段階までに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ガイド」がIPAから2013年に出されるなど(30)、セキュリティ強化のための取組が進められている。

(27) 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>
(28) 情報処理推進機構「繋がる組込みシステムの脅威とその対策」2014.7, p.4. <http://www.chubu.meti.go.jp/technology_jyoho/download/2014072425/2014072425ipa.pdf>
(29) 路車間通信は車両と路側機との情報のやり取り、車車間通信は車両同士の情報のやり取り。
(30)「“セキュアな自動車”に向けて「自動車の情報セキュリティへの取組みガイド」等を公開―企画段階から廃棄段階まで、自動車セキュリティを検討すべき15個のポイント―」2013.3.25. 情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/fy24/reports/emb_car/>

医療機器についても、セキュリティ上の脅威が顕在化しており、国内外でセキュリティインシデントが発生している。2011年のブラックハット（コンピュータセキュリティの国際会議）においては、インスリンポンプやペースメーカーなど無線通信を行うインプラント型医療機器に対して、ハッキングにより患者に対して致死性の攻撃を加えることができると指摘されるなど、患者の生命に関わるような重大なセキュリティ上の欠陥について指摘もなされている(31)。米国ではこれらの動きに対し、2013年に米国食品医薬品局（Food and Drug Administration: FDA）から医療機器のセキュリティに関するガイドラインや勧告が示されるなど(32)、医療機器のセキュリティに関する意識が急激に高まっている。日本においても、電子情報技術産業協会（JEITA）医療用ソフトウェア専門委員会や日本画像医療システム工業会（JIRA）、保健医療福祉情報システム工業会（JAHIS）などで医療情報システム及び医療機器のセキュリティについて検討が行われており、IPAも2013年には「医療機器における情報セキュリティに関する調査」報告書を公表するなど、医療機器のセキュリティに対して取組が進められている(33)。しかしながら、これまでの検討は医療情報システムのセキュリティが中心となっており、日本においても医療機器のセキュリティに関する検討や啓発活動が求められている(34)。

執筆：株式会社三菱総合研究所　情報通信政策研究本部　研究員　松本（まつもと）　尭（たかし）
監修：電気通信大学情報理工学研究科　教授　新（しん）　誠一（せいいち）

(31) Jerome Radcliffe,“Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System,”*Black Hat USA 2011*, August 2011. <https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf>; Daniel Halperin et al.,“Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses,”*Proceedings of the 2008 IEEE Symposium on Security and Privacy*, May 2008, pp.129-142.

(32) U.S. Food and Drug Administration,“Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff,”October 2, 2014. <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf>;“Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication,”June 13, 2013. U.S. Food and Drug Administration Website <http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm>

(33) 情報処理推進機構「医療機器における情報セキュリティに関する調査」2014.4.16, pp.32-41, 50. <http://www.ipa.go.jp/files/000038223.pdf>

(34) 同上, p.58-60.