特集　超スマート社会(Society5.0)に貢献する化学工学

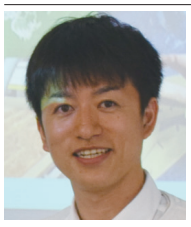
経済・社会が大きく変化する中で，新たな未来を切り拓いて国内外の諸問題を解決するためには，科学技術イノベーションを強力に推進していく必要ある。これに対し，政府の総合科学技術・イノベーション会議が2016年度から5年間の科学技術政策の基本指針「第5期科学技術基本計画」において，サイバー空間とフィジカル空間（現実社会）が高度に融合した「超スマート社会」の実現を目指した『Society 5.0』を提唱している。このような超スマート社会サービスプラットフォームの構築にはIoTシステム構築，ビッグデータ解析，AI等の科学技術の発展が必須であり，化学工学を含む様々な分野におけるこれら科学技術の活用事例，今後の展望について紹介する。　（編集担当：長田光正・古山通久・廣田淳一）†

「超スマート社会」におけるサイバー攻撃の脅威とセキュリティ対策

金子 晃介

1. はじめに

現代社会において，私たち人類は，日々の様々な場面でコンピューターの恩恵を受けて生活を営んでいる。特に，コンピューターを用いて利用するインターネットは，人類の情報伝達の速度を飛躍的に向上させ，私たちのライフスタイルやビジネスのあり方を大きく変化させてきた。今日，インターネットは，電気，ガス，水道に続く第4のインフラといっても過言ではないほど私たちの生活と密接に結びついている。そして今，このインターネットは，さらなるパラダイムシフトを迎えようとしている。すなわち，Internet of Things（以下，IoT）と呼ばれるコンセプトである。本稿では，IoTによる未来社会とその社会で必要とされるセキュリティ対策について考えていきたい。



Cyberattack Threats and Cybersecurity Measures on “Super Smart Society”
Kosuke KANEKO
2013年　九州大学大学院システム情報科学府博士後期課程単位取得退学
現　在　九州大学サイバーセキュリティセンター 富士通スペシャリスト育成研究部門　准教授
連絡先：〒819-0395　福岡県福岡市西区元岡744
E-mail　kaneko.kosuke.437@m.kyushu-u.ac.jp

2017年10月3日受理

2. IoTがもたらす「超スマート社会」

近年，IoTという言葉を情報学以外の様々な分野でも耳にするようになってきた。この章では，IoTに関する基礎的な知識や事例を説明するとともに，IoT技術が普及した先にある「超スマート社会」について紹介したい。

IoTとは，私たちの身の回りにある様々なモノがネットワークで接続され，モノとモノとが互いに通信をおこなえるような仕組みを指す言葉である。ここで言うモノとは，例えば，携帯電話，腕時計など小型なモノから，洗濯機，冷蔵庫，自動車などの大型なモノまでありとあらゆるモノを指している。このようなモノ同士のネットワーク環境を作り出すことで，私たちの身の回りのモノから様々なデータを収集し，取集したデータを人工知能（以下，AI）などの技術を活用して解析し，その解析結果を私たちのライフスタイルやビジネスにフィードバックすることで，より最適（スマート）な成果を得ることができると考えられている。このようなフィードバックをより意識したIoTの仕組みは，CPS（Cyber-physical System）とも呼ばれている。総務省が発表している情報通信白書によると，2020年には，世界のIoTの機器の台数は約304億台（平成28年度版）に，世界のIoT市場規模1.7兆ドル（平成27年度版）になるとの予想が記

† Osada, M.　平成29，30年度化工誌編集委員（1号特集主査）信州大学繊維学部化学・材料学科
Koyama, M.　同上　九州大学 稲盛フロンティア研究センター
Hirota, J.　同上　（株）カネカ 生産技術研究所

載されている[1]。このように，近い将来IoTは，私たちのライフスタイルやビジネスに大きな影響を与えると想定されている。

IoTを導入したサービスの例としては，家電製品にIoTの仕組みを導入したスマートハウスや産業用機器にIoTの仕組みを導入したスマートファクトリーや生活の基礎インフラやサービスにIoTの仕組みを導入したスマートシティなどが挙げられる。特に，スマートファクトリーに関しては，ドイツ政府が推進しているIndustrie 4.0と言う技術戦略が有名である。この名称には，産業の人類史に於いて，蒸気機関による第1の産業革命，電力による第2の産業革命，コンピューター制御による第3の産業革命に匹敵する第4の産業革命としてのIoTやAIに対する期待が込められている。Industrie 4.0の具体的な事例として，ゼネラル・エレクトリック社（以下，GE社）のデジタルツインと呼ばれるコンセプトが挙げられる。GE社では，航空機のジェットエンジンに取り付けられた大量のセンサーから得られるデータを利用して，高度なシミュレーションをおこない，その結果を現場にフィードバックすることで，エンジンの保守スケジュールの最適化や問題の兆候の早期発見に繋げている。その他の事例として，効率的なエネルギー管理にIoTを利用するエナジーマネジメントシステム（HEMS，FEMSなど）や効率的な農作物の管理にIoTを活用するなどの取り組みの事例が報告されており，様々な分野でのIoTの活用が始まっている[2]。

このようなIoTを活用した事例が普及し，私たちのライフスタイルやビジネスを最適に支えてくれる社会こそが，わが国が実現を目指している「超スマート社会」であろう。「超スマート社会」という言葉は，2016年1月に閣議決定された「第5期科学技術基本計画」の中に出てくる用語で，その定義は以下のようになっている。

「必要なもの・サービスを，必要な人に，必要な時に，必要なだけ提供し，社会の様々なニーズにきめ細かに対応でき，あらゆる人が質の高いサービスを受けられ，年齢，性別，地域，言語といった様々な違いを乗り越え，活き活きと快適に暮らすことのできる社会」

わが国では，このような「超スマート社会」を，狩猟社会，農耕社会，工業社会，情報社会に続く第5の社会として，Society 5.0と位置づけ，「超スマート社会」の実現に向けて，IoTやAIなどの情報通信技術を広い分野で活用した取り組みを始めている。

3. IoT時代におけるサイバー攻撃の脅威

前述の「超スマート社会」が実現した際には，製造業，農林水産業，医療，教育などの様々な分野で，私たちはIoTによる恩恵を受けることになるだろう。その一方で，普及したIoTサービスを狙って社会的な問題を引き起こすようなサイバー攻撃も増加する可能性が考えられる。この章では，IoT時代におけるサイバー攻撃の脅威について事例を交えながら紹介していこうと思う。

2016年10月に，IoT機器を狙ったマルウェアによる大規模なサイバー攻撃の事件が発生した。このマルウェアは，「Mirai」という名称で，ネットワークカメラや家庭用ルーターなどのIoT機器に感染し，特定のサーバーにDDoS攻撃を仕掛けるものであった。DDoS攻撃とは，標的のシステムに，一斉にアクセスすることで，システムに負荷をかけてサービスができないようにする攻撃である。つまり，このマルウェアに感染した世界中のIoT機器が，ターゲットとなったシステムに一斉に攻撃を仕掛けてきたのである。実際にこの攻撃は，ダイン社のDNSサーバーに対しておこなわれ，同社のDNSサーバーを利用しているAmazonやTwitterなどのサービスに障害が出たとの報告がされている[3]。DDoS攻撃自体は古くから存在するサイバー攻撃の一つではあるが，IoT機器が普及することで，この攻撃がさらに猛威を振るう可能性がある。なぜなら，私たちの身の回りにある様々なモノがネットワークに繋がるIoT時代には，これまでに類を見ないほどの数の機器がインターネットに接続されると想定されているからである。これら無数のIoT機器がマルウェアに感染し，一斉に攻撃を仕掛けてきた場合，その攻撃を防御するのは非常に困難であろう。実際に，前述のMiraiによるサイバー攻撃の事件では，ダイン社の報告によるとMiraiに感染した10万台以上のIoT機器から攻撃を受けたとの報告がなされている。

IoTが普及した社会では，様々な分野で，このようなサイバー攻撃が起こり得る可能性が考えられる。例えば，生活に関連する分野では，身の回りにある家電IoT機器から収集したデータを管理するサーバーがハッキングされて，個人情報が漏洩するなどの被害が考えられるだろう。農業分野では，農作物の管理に利用される室温，湿度，光量，水量などのセンサー機器が，サイバー攻撃を受けて改ざんされたデータを送り合い，農作物の生産性に影響が出るなどの可能性も考えられる。医療分野では，病院で利用されるIoT機器がマルウェアに感染することで重要な医療システムや環境システムに障害が出て，人命に関わる事故が起きる可能性も考えられる。実例として，2017年5月に流行した「WannaCry」というランサムウェアが，イギリスの医療機関のコンピューターに感染した事例が挙げられる。ランサムウェアは，コンピューター内のデータを勝手に暗号化し，暗号化されたデータの身代金を要求するマルウェアである。前述の事件では，管理しているコンピューターがランサムウェアに感染したため，コンピューターを利用した病理診断に影響が出たとの報告がなされている。また，製造業などの分野では，工場内のネットワークに繋がった

産業用機器が乗っ取られて制御不能になるなどの事件も想定される。実際の事例として，2010年9月に「Stuxnet」というマルウェアによって，イラン国内の核燃料施設で，ウラン濃縮用遠心分離機を制御不能にする事件が起こっている。

前述のように，IoTがライフスタイルやビジネスのインフラのように取り扱われる時代には，IoTサービスに対するサイバー攻撃の被害は甚大なものになる可能性がある。また，このようなサイバー攻撃に対する被害の影響は，システム自体も被害を受けるだけでなく，そのシステムを運用している組織自体の社会的信頼にも影響を与えかねない。組織の社会的信頼の失墜は，株価などに直接的な影響を与える可能性もあるため，組織にとって莫大な利益の損失につながり得る。サイバーセキュリティ対策は，「コストではなく投資」と言われる理由の一つはここにある。また，日本は，2020年に東京オリンピックを控えており，組織としてだけでなく，日本国としての国際的な信用を失わないために，日本全体でサイバーセキュリティ対策を意識して，国際的なサイバーテロに対抗していく必要もあるだろう。

4. IoT時代におけるセキュリティ対策

前節で説明したようなサイバー攻撃による脅威に対して，適切なセキュリティ対策をおこなっておくことは非常に重要である。しかしながら，情報セキュリティの分野に精通していない方にとっては，一体どこからセキュリティ対策を始めていけば良いのか戸惑うのではないかと思われる。そこでこの節では，情報学の学問の体系に倣ってセキュリティ対策について説明をしていこうと思う。

情報学の分野では，情報セキュリティの3要素と呼ばれているものがある。すなわち，「機密性（Confidentiality）」「完全性（Integrity）」「可用性（Availability）」の3要素である。この3要素は，古くから提唱されているコンセプトではあるが，近年の先端的なIoTの分野にも十分に適用可能である。この3つの要素を軸にセキュリティ対策の方針を決めていくやり方は，情報関係の組織では，よく実践されている手法である。

最初に「機密性」について説明しよう。「機密性」とは，ある情報資産に対してアクセスを認められたものだけが，その情報資産にアクセスできる状態を確保していることを指す。具体的な例で言うと，不正アクセスや盗聴に対する対策である。IoT機器が悪意のある攻撃者から不正にログインされた場合，そのIoT機器上でマルウェアなどを実行される危険性がある。また，IoT機器間で送信しているデータの内容を悪意のある攻撃者から盗聴された場合，盗聴されたデータの内容が解析されて，攻撃者にデータの改ざんやなりすましなどの次の攻撃段階への足がかりを与えてしまうことになる。不正アクセスに対する対策としては，認証が基本的な対策となる。例えば，IoT機器の工場出荷時の初期IDとパスワードで認証できるような状態で運用することは避けるなどが挙げられる。また，IoTサービスの基幹システムでは，二段階認証や多要素認証を利用するのも良いだろう。通信内容の盗聴に対する対策としては，暗号化された通信方法を使ったり，データの内容自体を暗号化したりすることで対策となる。特に近年，暗号化されていないTelnetでの通信を利用したIoT機器が問題になっているため，Telnetを利用した通信は避けた方が良いだろう。また，IoT機器自体が分解されたり，解析されたりするのを防ぐために，リバースエンジニアリングをされにくい仕組みやプログラムコードの難読化などを導入して，耐タンパー性を高めるのも良い対策になる。

次に，「完全性」について説明しよう。完全性とは，情報資産が，破壊されたり改ざんされたりすることなく完全に保たれている状態を確保していることを指す。具体的な例で言うと，通信内容の改ざんやプログラム自体の改ざんに対する対策である。IoT機器間での通信内容が改ざんされてしまうと，データの解析などに影響を与えてしまい，IoTを構成するシステム全体に大きな障害が出る可能性がある。改ざんに対する対策としては，ハッシュ値を用いた検証が有用だ。ここでの詳しい説明は避けるが，ハッシュ値の特徴を利用すると，データの改ざんを検知できる。ハッシュ値を利用した検証の応用性は高く，IoT機器のファームウェアのアップデート時などに送られてきたプログラムが改ざんされていないものなのかを検証したり，プログラムの起動時にプログラム自体が改変されたりしていないかを検証したりすることができる。このようなハッシュ値を利用した改ざん検出は，完全性におけるセキュリティ対策として非常によく利用される手法である。

次に，「可用性」について説明しよう。可用性とは，アクセスを認められたものが，常に情報資産にアクセスできる状態を確保していることを指す。具体的に言うと，システム障害などに対する対策である。前節での事例のように，IoTサービスが普及した社会では，IoT機器への攻撃が工場の生産性や医療現場での生命に関する被害に直結してしまう可能性がある。対策としては，システムをバックアップしておくなどが挙げられる。システムのバックアップがあれば，前述のランサムウェアのような被害にあったとしても，システムを素早く復旧させることが可能になる。また，ファイヤーウォールやIDS（不正侵入検知システム）やIPS（不正侵入防御システム）やWAF（Web Application Firewall）などを導入し，障害に強いネットワークを構成しておくことも対策となるだろう。

前述の情報セキュリティの3要素に止まらず，組織でさらに検討が可能な場合は，「真正性（authenticity）」「責任追跡性（accountability）」「信頼性（reliability）」「否認防止（non-repudiation）」の4要素を加えて，情報セキュリティの7要素

として対策を検討してみるのも良いだろう。特に，真正性で問われている「なりすまし」に対する対策は，IoT機器間でデータを受け渡す際に，本当に正しいIoT機器から送られてきたデータなのかを検証する工程で非常に重要である。「なりすまし」に対するセキュリティ対策としては，公開鍵暗号の仕組みを利用したデジタル署名による検証などが有用である。

前述で説明してきたようなセキュリティ対策をおこなうことは非常に重要であるが，セキュリティ対策をおこなえば，攻撃者からシステムを万全に守れるというわけではない。現代の社会において，万全なセキュリティ対策など存在しない。どんなセキュリティ対策も破られる可能性があると考えて，何重にもセキュリティ対策を施しておく多層防御の考え方が非常に重要になっている。また，セキュリティに対するインシデントは必ず起こるものだと想定して，インシデントが起こった際に対応するComputer Security Incident Response Team（以下，CSIRT）を組織内に配置しておくのが良いだろう。現在でも，多くの組織がCSIRTを配置し，日本シーサート協会などを通じて，組織の枠を超えてセキュリティに対する情報共有などをおこなっている。その他にも，組織内において，情報資産の管理やシステムの運用が適切におこなわれているかを調査するために，ISMS（Information Security Management System）に基づく監査などを定期的におこなうのも良いだろう。

セキュリティ対策の最後の項目として，最も重要だと思われる人材育成についても説明しておきたい。現在起こっているセキュリティインシデントの多くは人災によるものである。例えば，メールに添付しているマルウェアを起動してしまったり，重要なIDとパスワードをフィッシングサイトに入力してしまったりするなどが挙げられる。IoTのシステムに対して，前述のような様々なセキュリティ対策を施していても，運用する側の人間がセキュリティに対する知見がなければ，せっかく費用をかけておこなったセキュリティ対策も無意味なものになってしまう。近年では，攻撃者は，情報セキュリティの知識の乏しい人間を標的にして狙ってきているので，組織のセキュリティエンジニアだけでなく，組織の構成員全員で，その組織のセキュリティ対策に当たる時代になってきている。このような背景から，組織でセキュリティに対する意識を向上させるための教育や訓練をおこなうことは重要になってくる。例えば，情報セキュリティに対するeラーニングや標的型攻撃メールに対する訓練などを定期的におこなうことは，組織の構成員のセキュリティに対する意識を向上させる上で非常に有益である。また，組織の構成員に情報セキュリティに対する関心を持ってもらうために，組織内に最新のセキュリティ関連のニュースなどを閲覧できるポータルサイトを作るのも良いだろう。このような組織内におけるセキュリティ教育や訓練に対する活動も前述のCSIRTの役割となる。

5. おわりに

本稿では，IoTがもたらす未来社会の展望について紹介すると共に，IoT時代における脅威とそのセキュリティ対策について説明してきた。

本稿であげてきた情報セキュリティの対策は，基礎的な対策ばかりであり，IoT時代におけるセキュリティ対策のほんの一例にすぎない。紙面の都合上本稿では，取り上げることができなかった様々な対策があるので，情報セキュリティに対して興味を持たれた方は，是非書籍やインターネットなどを活用して詳しく調べてみてほしい。また，前述の通り，サイバー攻撃での被害は，システムに対する直接の被害だけでなく，その組織の社会的信頼を失墜させ，莫大な利益の損失につながる可能性がある。そのため，これからの社会の情報セキュリティは，セキュリティエンジニアだけでなく，組織の構成員全体で対策に当たらないといけない時代に突入している。つまり，組織の構成員全員がセキュリティに対する基礎的な知見を身につけておく必要がある。さらに，組織のCSIRTやCIO，CISOを担当されている方々は，適切に組織で運用するシステムの情報セキュリティ対策について，組織内での予算等を考慮に入れながら，どこまでセキュリティ対策をおこなっていくべきかの判断をできる能力を身につけておく必要があるだろう。情報セキュリティ対策は，多層に考慮しておく必要はあるが，費用面とのバランスも考える必要がある。また，IoTのシステムの導入や運用に際して，設計や導入段階から情報セキュリティを考慮して，設計や開発に対する物事を判断できる人材が必要になって来ている。このような考え方は，セキュアバイデザイン（Secure by Design）と呼ばれており，近年，重要なコンセプトになって来ている。

2018年を迎えた今，近い将来訪れるであろう「超スマート社会」に向けて，化学工学の分野全体で，「IoTと情報セキュリティ」にどのように向き合っていくのかを考えていく時期に来ているのかもしれない。5年後，10年後先の化学工学の分野に，どのような未来のビジョンを描いて，それをどう実現していくかの方針を決めるのは，今まさに化学工学の分野を担っている方々の役割である。そのビジョンを実現するために，学問の垣根を超えて，情報学の分野からも様々なディスカッションをおこなっていければ，そのような活動が，化学工学と情報学の両分野のさらなる発展につながると信じている。

参考文献

1）総務省：情報通信白書　http://www.soumu.go.jp/johotsusintokei/whitepaper/
2）すべてわかるIoT大全2017，日経BP社（2017）
3）YOMIURI ONLINE　http://www.yomiuri.co.jp/science/goshinjyutsu/20161028-OYT8T50051.html