IoTに対するセキュリティーの考察

安全で安心なサイバー社会を目指して

次世代サイバー空間の中で、IoT(Internet of Things)は重要な役割を果たすことになります。しかし、そのIoTを活用する新サービスや接続形態の中には、新たな脅威やリスクが内在しています。本解説では、IoTを取り巻く具体的なリスクの実例を紹介し、近未来に直面するであろうセキュリティーについての問題提議を行います。また、その問題を解決するための手法、IT環境で培ったセキュリティー対策の知見を活用する方法論を解説します。

安全・安心なサイバー社会を実現するために、今こそがIoTが抱えるセキュリティーの課題を正しく理解し、長期的なビジョンに基づいた対策を始める時なのです。

1. IoTに対するセキュリティーの必要性

窃盗団が豪邸への電源供給を止める、テロリストが監視カメラの映像を書き換えモニターで監視中の警備員をだます、ハッカーが走行中のバスを遠隔操作する――映画でこのようなシーンをご覧になった読者も多いと思います。皮肉にもIoTの発達により、映画の世界の脅威が、現実社会にもたらされる可能性が出てきました。

実社会ではすでに、電源管理の一部がスマート・メーター機器経由で行われ、スマート・ホーム用の家電、町中の監視カメラや自動車はネットワーク経由で各種センターにつながっています。閉じられた世界で利用されていた機器がインターネットにつながる、いわゆるIoT化したことで、理論的には新たな火種を抱えることになるのです。IoTの時代は、悪意を持った攻撃者に対して裏口(バックドア)が開放された時代とも言い換えられるのです。また、そのIoT機器に組み込まれたソフトウェアも、独自性の強いものからLinux、Android、Windows OSという汎用的なものに変化してきています。これは攻撃者にとっては、ITシステムで培った攻撃に関する知識やクラッキング・ツールが再利用可能であることを意味します。

本解説では、汎用的なソフトウェアを搭載し、インターネットにつながったIoTが直面するセキュリティーの課題を紹介します。また、Systems of Engagement (SoE:協働のための情報活用システム)の重要な構成要素であるIoTのセキュリティーを確保することが、SoE時代に安全にかつ安心してそのサービスを享受することにつながるのです。

2. 情報セキュリティーとIoTセキュリティー

一般的な情報セキュリティーはCIAと呼ばれる「機密性(Confidentiality)」「完全性(Integrity)」「可用性(Availability)」を基本理念にしています。CIAを保証・担保するために認証、認可、監査、脆弱性対策などの要素技術を配置し、サービスの継続性、重要情報を保護しています。IoTがエンドポイントとしてITシステムの一部となるとき、またはIoTの特性を活かした全く新しいサービスを提供する場合には、ITシステムと同等のセキュリティー対策が必要になるはずです。

ただ現時点において、IoTに対するセキュリティーの必要性や認知度は、業界によって温度差があるのが実情です。日本でも導入が決定しているスマート・メーターに関しては、NIST(National Institute of Standards and Technology)からガイドラインが発行[1]されており、具体的なセキュリティー対策が検討されています。また、自動車業界では欧州が主導して行ったEVITA(E-safety Vehicle Intrusion proTected Applications)プロジェクトによる報告書[2]、IPA(情報処理推進機構)が発行し

た「自動車の情報セキュリティへの取組みガイド」[3]を参考に、各社準備を進めている状況です。

では、セキュリティーへの取り組みが遅れているIoTを有する業界は、どのように対策を進めるべきでしょうか。セキュリティーの世界では、業界のガイドライン・標準を順守することは重要な意味を持ちます。前述のガイドライン等は、想定されるリスクの洗い出し、リスク分析の手法、セキュリティー要件の整理の仕方が記述されています。その内容は業界の枠を超えて、いかにIoTのセキュリティーと取り組むべきかを考察する上で一読の価値があるものです。物理的な設計方法、対策の粒度感は違っても、後発業界が参考にできる内容が多数あると考えてよいと思います。

3. IoTセキュリティーの現状と課題

一概にIoTといっても、対象になる機器や接続するシステムはさまざまであり、その利用用途によって、セキュリティーの必要性は異なります。IoTのセキュリティー強化を考える上での制約事項を**表1**にまとめます。要約すると、ビジネスの観点から言えば、高価な制御機器の類には投資できても、消費者向けのウェアラブル・デバイスや電気機器などには、その必要性を感じていません。技術的には、IoTに適用できるセキュリティー技術が十分に成熟、流通していない課題も抱えています。例えば、IoT内部が独自の通信プロトコルを採用している場合、TCP/IPを前提としたファイアウォールやIPS(侵入防御システム)の技術をそのまま適用することが難しい、ということです。よって、IoTのセキュリティーを考える場合、IoTがもたらすビジネス的価値、技術の成熟度などを見極めることが重要になります。

表1. セキュリティーに関する制約事項

	制約事項
ビジネス的側面	・IoTに対するセキュリティーの必要性が理解できていない ・法律による規制、業界のガイドラインが整備されていない ・IoT自身が安価なため、セキュリティー対策への追加投資が難しい ・保護すべき価値が存在しない／微少である ・セキュリティーを理解した設計者、製造者、サプライヤーが少ない
技術的側面	・漠然とした不安はあるが、どのように着手するのか分からない ・どういったリスクが存在するのか分からない ・どういったセキュリティー技術が必要なのか分からない ・サイバー・リスクがIoTの品質にどういった影響を与えるのか不明瞭である (リスクが内在しても、品質が変わらなければ大きな問題ではない) ・独自性が強いアーキテクチャーのため、適用できるセキュリティー技術が少ない

本解説では、具体的な例として、比較的セキュリティーの必要性が高く、筆者の経験値が高い自動車を題材にすることにします。近年の自動車は「つながる車」(Connected Car)とも呼ばれ、自動車内部で収集した情報をデータセンターに送ることで、遠隔診断、エコ運転評価、対話的ナビゲーションなどのサービスを提供します。この情報の中には、GPS位置情報や運転履歴といったプライバシーに関する個人情報も含まれるため、「機密性」の確保が必要になります。次に、将来的に自動運転システムを効果的に支援するためには、自分以外の自動車やITS(Intelligent Transport Systems)から送られた情報が必要になります。もし、その情報が改ざんさ

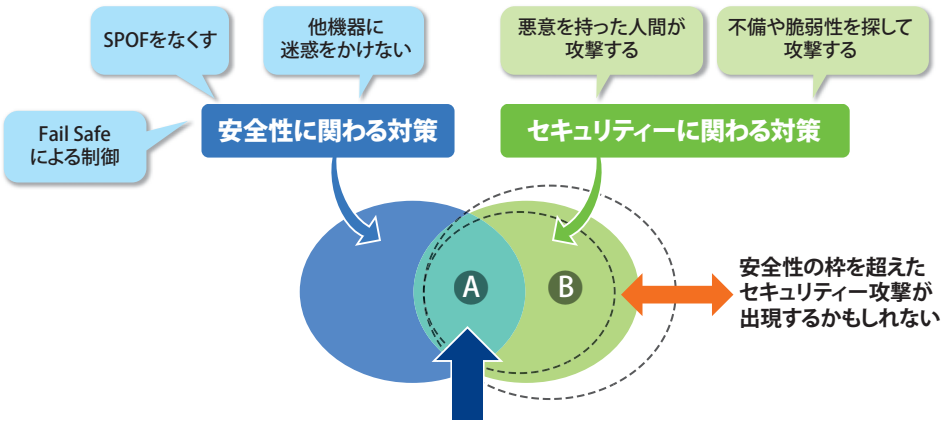

図1. 安全性とセキュリティーの関係

れており、「完全性」が保証されない状態であった場合、正しい計算・処理を行うことが難しくなる危険性があります。また、車載コンピューター(ECU:Electronic Control UnitまたはEngine Control Unit)のソフトウェアに脆弱性があり、内部の通信の遅延、駆動装置の誤動作が発生した場合、自動車の安全な走行という「可用性」に影響が出るかもしれません。つまり、つながる車がその付加価値サービスを提供するためには、セキュリティーのCIAの確保が不可欠なのです。

では、セキュリティーの考慮が不十分な自動車は危険な状態で走行しているのでしょうか？　少なくとも現時点では、犯罪者が自動車を乗っ取り、遠隔操作したという事件の報道はないと思います。しかし学術業界では、米ワシントン大学と米カリフォルニア大学サンディエゴ校の研究者が2010年にECUへの不正アクセスが可能であり、システムの安全機能プログラムが改ざん可能であることを実演で示しています[4]。近年では、Black Hatコンファレンス[5]において、自動車に対する攻撃例が紹介されたことで、IoTに対するセキュリティーが大きな関心を集めるようになりました。ハッカーにとって、名声を上げる垂涎の的がIoTに対するセキュリティー攻撃の実証である、と2013年のBlack Hatコンファレンスにおいて講演されています。われわれが留意すべき点は、高度なセキュリティー技術者や攻撃者がIoTに興味を持ち、次のサイバー攻撃の対象として、IoTを観察しているという状況を認知しておくことです。

図1は自動車会社における、安全性とセキュリティーの関係を表しています。自動車会社は品質管理の一環として、安全性を追求しています。1カ所の部品の故障や組み込みソフトウェアの不具合が自動車全体に影響しないために、Fail Safeという考え方の元に多段的な対策を講じており、SPOF(Single Point of Failure)をなくし、安全性を保証しています。この徹底した安全性の取り組みによって、たとえ内部に不具合、脆弱性が見つかったとしても、自動車全体に大きな影響は発生しない、と考えられています。一方、セキュリティー対策とは、攻撃者が悪意を持って、仕様の不備に対する攻撃を行っても、CIAを保証するための対策です。例えば、部品の故障などでは起こり得ない膨大なデータ量を意図的に発生させ、仕様を超えた量のデータを頻繁に送信し、駆動装置を混乱させる攻撃(ITシステムでは有名なDoS:サービス妨害攻撃)にも対応しなければなりません。現時点で、

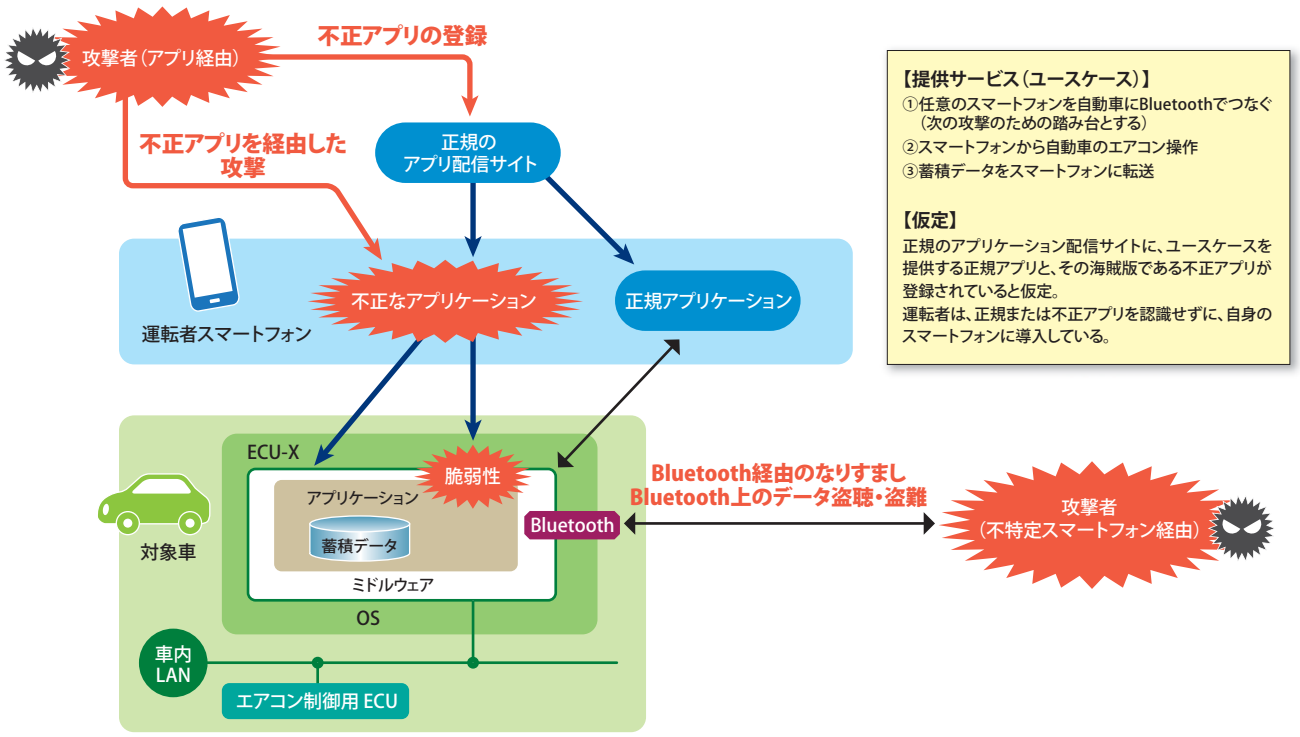

図2. ユースケース

IoTのセキュリティーが大きな社会問題になっていないことを考えると、**図1**のセキュリティーの部分が安全性の円の中に吸収されてきた（Ⓐ部分）と考えることができます。しかし今後は、攻撃者は安全性の円に納まらないセキュリティーの部分（Ⓑ部分）に属する攻撃を行ってくるでしょう。サイバー攻撃とは、言い換えれば、想定外の部分を狙った攻撃そのものなのです。

4. IoTセキュリティーのユースケース

ここでは、自動車を取り巻くリスクについて考えるために、スマートフォンと自動車をつなぐことで起こりえるリスクについて考察してみます。より現実的な問題を考えるために、昨今問題となっている、スマートフォン上の不正なアプリケーションも考察対象とします。

図2を参照してください。自動車のエアコンをスマートフォンから操作する、自動車の走行状況をスマートフォンに表示させるユースケースを題材にします。このサービスを提供するためには、自動車が外部のデバイスから制御系のコマンドを受け入れる、自動車内部に蓄積されたデータを外部に送信する必要が生じます。このサービスをセキュリティーの観点で整理したものが**表2**です。

表2. ユースケースに対するセキュリティーの整理

ユースケース	攻撃発生元	攻撃方法・内容	対抗策
①任意のスマートフォンを自動車にBluetooth でつなぐ（次の攻撃のための踏み台とする）	Bluetooth(BT)	BT経由のなりすまし	・ペアリング時の機器認証 ・データ交換前の利用者認証
		BT上のデータ盗聴・盗難	・データの難読化または暗号化 ・認証結果に基づいたデータへのアクセス権限設定
		BTファームウェアの脆弱性攻撃	・適切な脆弱性検査及びパッチの適用
②正規のスマートフォンから自動車のエアコン操作	正規のスマートフォンに導入された「不正なアプリケーション」	不正なアプリケーション経由で遠隔操作	・スマートフォン・アプリケーションと自動車内アプリケーション接続時の認証 ・スマートフォン上のセキュリティー・ソフトウェアによる挙動監視・防止
	上記の「不正なアプリケーション」と自動車内アプリケーションの脆弱性	自動車内部への侵入	上記に加えて、 ・自動車内アプリケーションの脆弱性に対する脆弱性検査 ・ECU－X上でのフィルタリング（許可された操作のみを享受）
		自動車内部の蓄積データ消去	・蓄積データのアクセス権限設定（ECU-X以外からの操作禁止） ・蓄積データのバックアップ
③蓄積データをスマートフォンに転送	正規のスマートフォンに導入された「不正なアプリケーション」	不正なアプリケーション経由でデータを外部転送	・スマートフォン・アプリケーションと自動車内アプリケーション接続時の認証 ・スマートフォン上のセキュリティー・ソフトウェアによる挙動監視・防止 ・蓄積データの難読化・暗号化（指定アプリケーションのみでアクセス可能）

表2には前述のユースケースに加えて、近年の自動車が標準的に提供しているBluetooth機能のセキュリティーにも言及しています。従来、あまり問題とならなかったBluetooth機能も、自動車がスマートフォンとつながるという新しいサービスが提供されるときには、安全を脅かす裏口になるかもしれないのです。**表2**はこのユースケースに対して、想定される攻撃の発生元、攻撃の方法と内容、およびその種の攻撃を軽減、防御するための対抗策を記述しています。

IoTセキュリティーの一番目の考慮点は、IoTがモビリティー機能、通信機能を前提とした機器であるということです。ITシステムの場合、データセンターやオフィスで利用する機器は物理的に隔離されており、接続先もある程度限定的です。これに対して、代表的なIoTである自動車やスマートフォンには物理的空間の制約はありません。また、近年の自動車やスマートフォンにはBluetooth機能が標準装備されています。Bluetoothはペアリングさえできてしまえば、理論的には交換するデータの漏えい、盗聴が可能な通信手段です。つまり、IoTセキュリティーでもっとも考慮すべきことは、不特定多数の人間、デバイスが容易に接続してくるリスクを有している点です。

二番目の考慮点は、過去のアーキテクチャー（設計思想）と「つながる」機能を融合した時に必要となるアーキテクチャーの見直しです。古い自動車は不特定の外部機器とつながることをあまり想定しないで長年設計、製造されてきました。このユースケースの場合、エアコン制御用のECU-Xにコマンドを送信できる仕様であるため、万一ECU-Xが乗っ取られた場合、車内LANに対するDoS攻撃、ECU-Xに蓄積されたデータの消去など、二次的な被害が発生する危険性が伴います（注記：筆者の知っている事例では、ECU-Xが乗っ取られた場合を考え、車内LANに攻撃できない特別な対策が実施されていました）。つまり、古いアーキテクチャーを有した製品に、

新しい機能を後付けで追加した場合、そこで発生しうるリスクには無防備かもしれない、という点です。

三番目の考慮点は、接続した相手が異常であるかもしれないリスクです。これは保証の範囲外だと考える読者もいるかもしれませんが、自身のインフラ、アプリケーションに脆弱性がなくても、接続先がなりすまされていたり、脆弱性を有していたりすることも起こりえます。このユースケースでは、リスクを有したスマートフォンが接続することを考慮しました。すなわち、正規アプリケーションに似た不正なアプリケーションが導入されており、それを経由してリモート攻撃が行われるケースを想定しています。

ITシステムのセキュリティーを担当されている方は、上記三つの考慮点に違和感をもたれるかもしれませんが、従来の固定概念を打ち破った柔軟な思考こそが必要になります。そして、IoTのセキュリティーを整理する上で、どこに保護すべき資産があり、どこを発生元に、どういった種類の攻撃を受けるかを整理するうえで、ユースケース図に従いリスクを洗い出していくことが、ステークホルダーの理解を高めるために有効なのです。

5. IBMの提言

この章では、IoTに対するセキュリティー強化に向けたIBMの提言を行います。

ITシステムでは、SE(システム・エンジニアリング)の工程で、常にセキュリティーの意識を持つことで、システムの強度を高めています。**図3**に事件、事故につながる可能性のある過失、ミスを例示しました。**図3**を見れば、IoT固有の問題はほとんどなく、ITシステムと共通の考え方であることが分かります。つまり、IoTのセキュリティー強化のために、全く新しいプロセス、仕組みを考えるのではなく、ITシステムでの経験値を活用すべきなのです。前述したNISTのガイドラインでも同じような手法を採用しています。IoTによっては、今後一層接続先の増加、サービスの拡充が期待され、ユースケースも複雑化してきます。しかしながら、各ユースケースに対して網羅的なリスクを整理するSE手法の基本を繰り返し、実践していけばよいのです。

あえてIoT固有の強化点を挙げるとすれば、設計段階におけるセキュリティー意識の醸成と製品出荷後の運用・管理方法の整備です。

(1) 設計段階におけるセキュリティー意識の醸成

サイバー攻撃に強いIoTを製造するためには、**図3**の「デザイン」工程の前にリスクを正しく認識し、セキュリティーを意識しておくことが重要です。発注者、サプライヤーとも、旧来の安全性の視点に加え、**図1**で示したセキュリティーの領域についても考慮しておく必要が

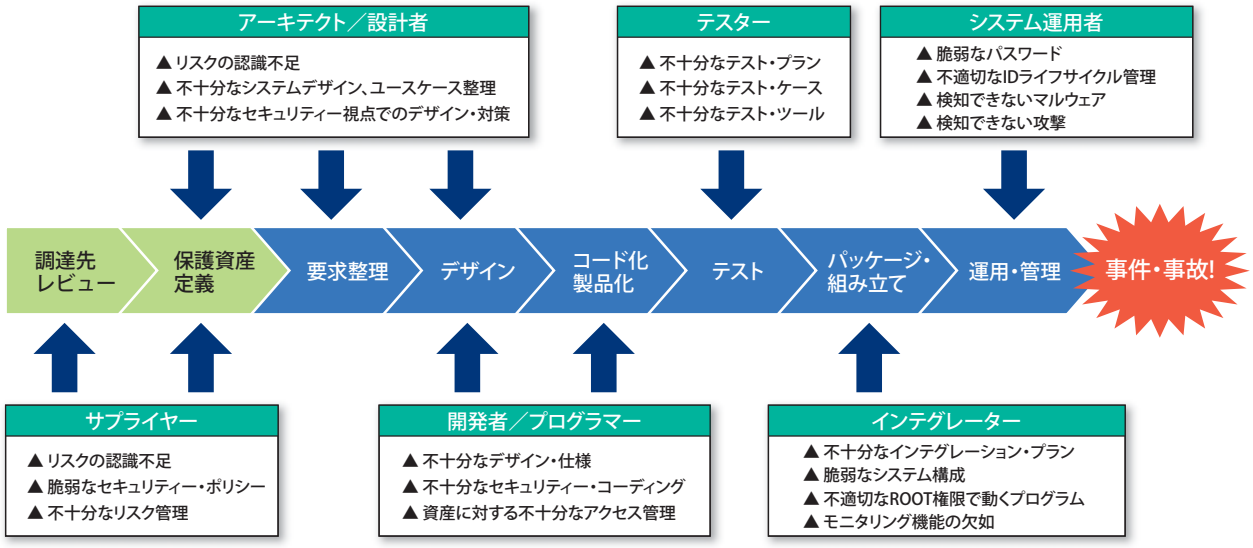

図3. セキュリティー工程の不備

あります。セキュリティーにおいても、PDCA（Plan-Do-Check-Act）ライフサイクル管理の中で、最初のPLANが重要であることは言うまでもありません。特に、未確定要素の多いIoTの場合、「保護資産定義」から「デザイン」工程を確実に行うことが有効な対策だと考えます。

（2）出荷後の運用・管理

現在のIoTで一番難しい対応が、出荷後の「運用・管理」です。IoTで重要なサービスを提供しているにもかかわらず、サイバー攻撃を受けた履歴を掌握できない、組み込みソフトウェアやアプリケーションが停止していても気付かない、ということはないでしょうか。これは技術的な制約ではなく、そのようなモニタリング機能をIoTでは必要だと考えてこなかったことが一因です。同様に、不具合、修正が起こったときに、遠隔から修正、保守する仕組みを作ること、それを実現する技術を開発することも今後の課題といえます。モバイル端末の流通に伴い、IT市場ではMDM（Mobile Device Management）、MAM（Mobile Application Management）、MCM（Mobile Content Management）といったモバイル端末管理ソリューションが台頭しています。このソリューションをIoTの独自プロトコルやアーキテクチャーとうまく融合できれば、IoT機器に対しても統合的な管理が可能になります。PDCAライフサイクルでのセキュリティー強化を実践するためにも、出荷後にACTできる仕組み、技術を準備しておくことが必要です。

6. 終わりに

IoTが流通、定着した新しい時代に、斬新なサービスを享受しながら、安全で安心な社会を実現するための考察を最後にまとめます。

まず、IoTを一意的に捉えず、その特性、仕様用途に適合したセキュリティー対策を講じるべきです。前述したCIAの要件をどこまで担保、保証すべきかを整理し、IoTがもたらす付加価値・サービスと内在するリスクを比較検証してください。つまり、遠隔医療・手術や自動運転システムなど人命にかかわるIoTシステムには、IoT機器の安全性に加え、高度なセキュリティー対策を実施します。一方で、ウェアラブル・デバイスのように快適性、利便性を追求するIoT機器には、プライバシーの保護だけは最低限保証する、といった濃淡のついたセキュリティー対策が必要です。

次にリスク対策には、IoT機器単体で解決すべき方法と、「IoTシステム」としてIoT機器を含んだアプリケーション、インフラ、接続するITシステム全体で解決すべきものに区分します。セキュリティーはエンド・ツー・エンドで考えるべき要件であるため、IoT機器単体のセキュリティー技術が成熟するまでは、補完的な役割として、IoTシステムとして鳥瞰的にCIAの担保を行うのが現実的な解決策です。

最後に、常にセキュリティーの重要性を意識しておくことです。留意しておくべき点は、リスクを検知する仕組みや軽減する方法がなく、結果としてリコールのような物理的な交換以外になすすべがない、という融通の利かないIoTを作ってしまわないことです。現時点で、効果的なセキュリティー技術の適用が難しいことは承知しています。しかし、長期的な計画の中で、ITシステムで経験した知識、仕組み、技術の組み合わせを考え、IoTシステムの堅牢化に取り組んでいくべき時を迎えていると考えます。

［参考文献］

[1] NIST：Guidelines for Smart Grid Cybersecurity, 入手先<http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>（2014）

[2] EVITA：EVITA Project, 入手先<http://www.evita-project.org/>（2014）

[3] IPA：自動車の情報セキュリティへの取組みガイド，入手先<http://www.ipa.go.jp/security/fy24/reports/emb_car/>（2013）

[4] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno,S. Checkoway, D. McCoy, B. Kantor, D. Anderson,H. Shacham, and S. Savage: Experimental security analysis of a modern automobile, *Proc. IEEE Symposium. SP*, pp. 447–462（2010）

[5] Black Hat Conference, 入手先<https://www.blackhat.com/us-14/>（2014）

日本アイ・ビー・エム株式会社
グローバル・テクノロジー・サービス事業
ITSデリバリー
ディスティングイッシュト・エンジニア（技術理事）

大西 克美
Katsumi Ohnishi

1986年日本アイ・ビー・エム入社。IBM Academyメンバー。IPSJ正会員。大学、研究機関担当のエンジニアとして、UNIXシステム、インターネット基盤のプロジェクトを担当。2000年前半より、ITセキュリティーのアーキテクトとして、金融機関等のコンサルティング、アーキテクチャー設計などで活躍。日本アイ・ビー・エムにおけるセキュリティーの第一人者として、講演、政府活動、執筆活動など幅広く活躍中。現在はグローバル・チームの一員としてサイバー攻撃対策を中心に活動中。