IoTセキュリティを支える「暗号技術によるトラスト」の重要性

JNSA PKI相互運用技術WGリーダ
セコム株式会社 IS研究所
松本　泰

1. はじめに

昨今、IoTの取り組みに対する世の中の関心の高まりに合わせて、情報セキュリティ業界においてもIoTのセキュリティに関する関心が高まっています。そもそもバズワードとも言えるIoTは、その定義自体が曖昧であり、その曖昧なIoTのセキュリティとなると更に曖昧となります。しかしながら、情報セキュリティ業界の一般的な意見としては、IoTが真っ当になるためには、セキュリティの対応が大変！そんなに甘くない！といった意見が、多数を占めるのではないではないでしょうか。

こうした中、将来に数百億個にものぼると言われるIoTデバイスやそれらから構成されるシステムの運用において、その脆弱性対応に翻弄されないためには、脆弱性を最小限にするためのIoTデバイスやそれらから構成されるシステムの設計時における「セキュリティ・バイ・デザイン」の取り組みが重要になると考えられます。そのセキュリティ・バイ・デザインにおいて、IoTのセキュリティのベースとなる機能の多くは、暗号技術により実現されると考えられますが、その一方、実装上において脆弱性を生みやすい部分自体も、暗号技術の実装部分だと考えられます。

暗号技術をどのように利用するかは、ビジネス面からみても重要な課題になります。大量のセンサーやアクチュエータ等のIoTデバイスと多様なクラウドサービスが連携するシステムによって提供されることが想定されているIoTによるサービスでは、ステークホルダー間の多様な信頼関係を構築できる必要があります。IoTデバイスから構成されるシステムにおいては、この多様な信頼関係構築のために暗号技術による「認証」「署名」等を使い、秘匿性の確保やサービスの分離のために「暗号化」を使ってこれらの課題を解決することは不可欠です。また、IoTデバイスのプログラムの更新時においても、そのプログラムの検証が暗号技術より行われると考えられます。

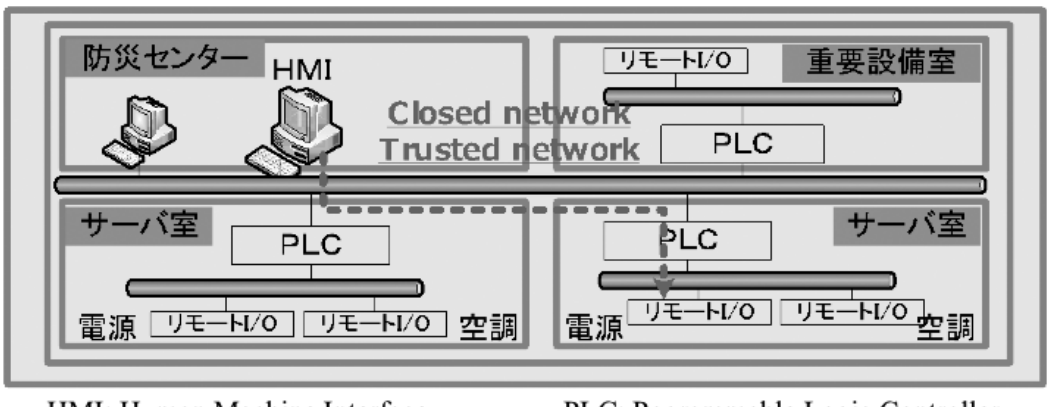
本稿では、こうしたIoTセキュリティのベースとなる機能等を「暗号技術によるトラスト」として捉え、その取り組みの重要性を解説します。

2. 重要インフラにおける物理セキュリティ環境によるトラスト

本題のIoTにおける暗号技術、および暗号技術によるトラストの話に入る前に、暗号技術があまり利用されていない重要インフラの制御システムにおける物理セキュリティ環境によるトラストについて説明します。

ここでは、重要インフラにおけるセキュリティのベースとなるトラストを説明するために 図1に示すデータセンターにおける電源や空調の制御をおこなうビルオートメーションシステムを想定して説明します。

今日において、多くの重要インフラの制御システムおよびそのネットワークは、堅牢な重要施設おける物理的



HMI: Human Machine Interface　　PLC: Pogrammable Logic Controller

図1　ビルファシリティネットワークのイメージ

なゾーニング等よる「強い物理セキュリティ環境」と人の運用により基本的なトラストが構成されていると考えられます。図1の例では、空調の制御に使われる防災センターとサーバ室間のビルオートメーションシステムのネットワークに、HMI（Human Machine Interface）としてPCのコンソールが接続されています。多くの場合、このHMIへのログインにはパスワードが必要になり、また、このPCから他の機器への通信ではBACnet等の標準化されたプロトコルが利用されていますが、そこには暗号技術による認証等は限定的にしか実装されていないのが実情のようです。そのため、このビルオートメーションシステムのネットワークを守るためには、物理的にネットワークを隔離する「物理セキュリティ環境」を構築する必要があります。そして、この物理セキュリティ環境によって隔離されたネットワークは「トラステッドネットワーク」と呼ばれています。

こうした状況の中、近年、重要インフラの制御システム、制御ネットワークへのサイバー攻撃が現実のものになりつつあり、それには以下のような背景があると考えられます。

(1) 重要インフラにおける制御システムの標準化、汎用化、コモディティ化
(2) 重要インフラの制御システムにおける様々な情報連携の要求
(3) 制御システムへの攻撃手法等の拡散

従来からの重要インフラにおける制御システムのクローズドネットワーク／トラステッドネットワークにおいては、隔離されたネットワークがそのセキュリティの前提になっていたため、そのボーダ（物理的なボーダ＆論理的なボーダ）を突破されると非常に脆弱という問題が浮上しています。

こうした問題に対応する動きの一つに、「日本データセンター協会」と「東京大学グリーンICTプロジェクト」が共同で設立し、筆者も副査として活動している「ファシリティ・インフラＷＧ[2]」の活動があります。この「ファシリティ・インフラWG」では、ビルオートメーションシステムの一層の活用を目指し、データセンターをこうした技術の先進的利用者と位置付け活動しています。

ファシリティ・インフラWGでは、活動を始めるにあたってビルディングオートメーション技術の導入ステージについて、図２にある3つのフェーズに分けて議論を行うことにしました。その最初のステップとして、これらのうちフェーズ１に対応したビルディングオートメーションシステムの設計・運用の為のガイド「建物設備システムリファレンスガイド [3]」(以下、リファレンスガイド)を2015年12月、内部向けに発行しています。

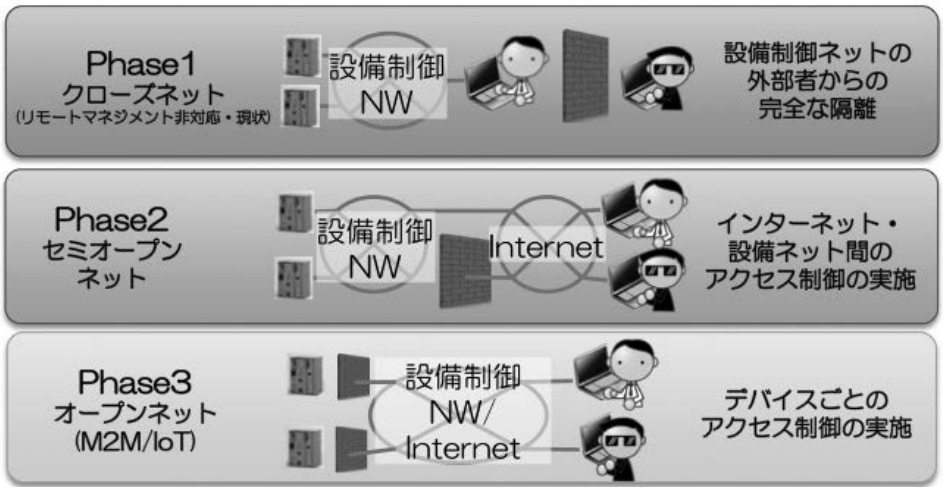


図2　ビルファシリティネットワークの３つのフェーズ

リファレンスガイドでは、ビルオートメーションシステムのネットワークを適切に外部から隔離することによって、システムのトラストを確保することを目指しています。そのため、リファレンスガイドで紹介しているセキュリティ管理策の内容は、適切な物理的ボーダー設計・構築方法や、その物理セキュリティを担保する運用方法となっています。このようなボーダーによる区画は、その構築・運用が比較的容易ではあるものの、前述したようにボーダーを突破されると非常に脆弱であるという課題があり、また、運用時における自由度にも課題があります。

そこで、フェーズ3において目指されているのが、より発展的なビルディングオートメーションシステムのあり方として「物理セキュリティ環境によるトラスト」だけに頼らない「暗号技術によるトラスト」の実現を目指したビルディングオートメーションシステムということになります。そして、図2において示したように、フェーズ3のビルディングオートメーションシステムはまさしくIoT時代におけるビルディングオートメーションシステムと言えるものになります。

3. IoT における暗号技術によるトラスト

センサーやアクチュエータ等のIoTデバイスとネットワークが、物理セキュリティ環境に依存しない場所おいて動作可能となると、それは、様々なイノベーションをもたらすと考えられます。そして、その際「物理セキュリティ環境によるトラスト」に代わって必要になるものが、「暗号技術によるトラスト」であると言えます。

ビジネス／サービスの観点から見たIoTシステムでは、様々なステークホルダーも含めた信頼関係（トラストモデル）を構築する必要があります。この信頼関係の構築は、主に暗号技術で利用される暗号鍵の関係性等により実現します。こうしたことも含めて、暗号技術は、IoTのセキュリティだけではなく、IoTにおけるビジネス自体の実現またはIoTによるイノベーションにとって必須な技術であると考えられます。

図3は、IoTではなく、現状のインターネットサービスのイメージで、ビジネスレイヤーにおいて顧客とサービス間のトラストをつくるために実際はどのような仕組みが取り入れられているかを説明した図です。インター

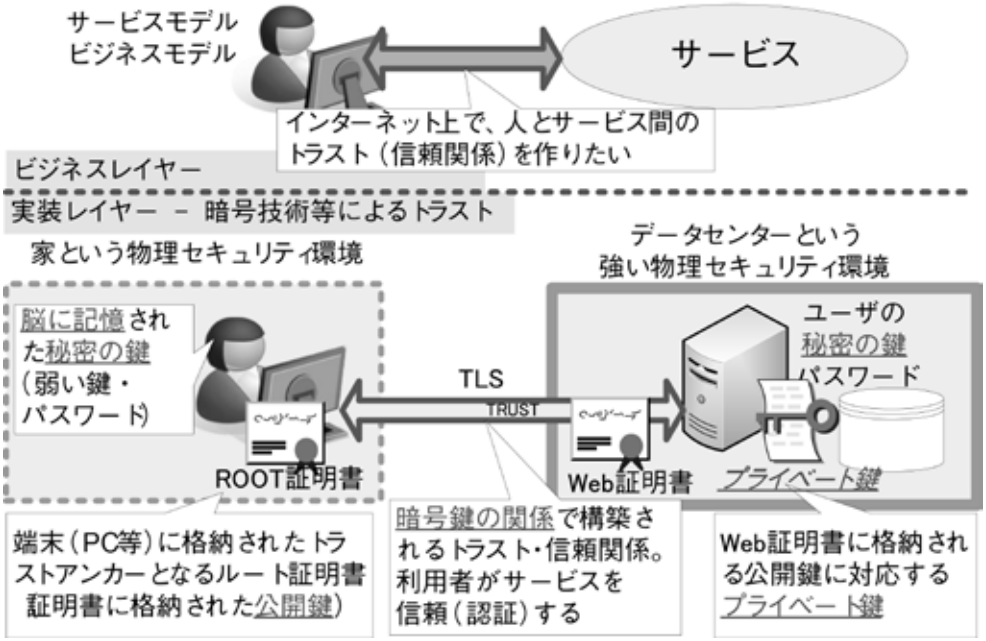


図3　インターネットにおけるサービスと暗号技術

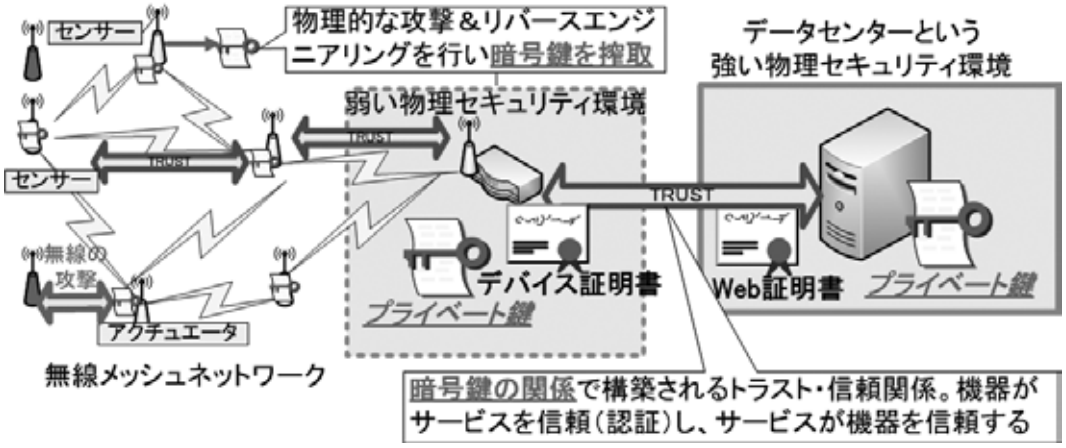


図4　IoT サービスと暗号技術

ネット越しのサービスにおいて、ビジネスレイヤーにおける信頼関係は、暗号鍵の配置等により決定される暗号技術によるトラストにマッピングされます。

このように、インターネット上のサービスにおいて、暗号技術はごく普通に利用されていますが、トラストは暗号技術だけで達成されている訳ではありません。例えばパスワードというものは人の脳に記憶された秘密の鍵を使います。また、PCは、オフィスといった物理セキュリティ環境に設置されます。センター側の暗号鍵にしても、それは（情報システムの）情報セキュリティだけで守っているわけではなく、物理セキュリティ環境でも守っている訳です。

これに対して図4は、IoTサービスをイメージした例になります。大量のIoTデバイスを接続するラストワンマイル、ラストワンメートルにおいて、その設置の自由度等の理由により無線通信を利用する場合、物理セキュリティを施すことが難しい為、必然的に暗号技術によるトラストが重要になります。また、IoTデバイスが、「弱い物理セキュリティ環境」において多く利用されることを想定した場合、物理セキュリティ環境も含めた「暗号鍵」の保護に代わって、IoTデバイス自身のハードウェアによる「暗号鍵」の保護の重要性が浮上します。さらに、数百億のIoTデバイスを想定した場合、その鍵管理等を人の記憶に頼ることはできませんから、そのためにもIoTデバイスに対した発行されるクレデンシャル管理や暗号鍵管理のための技術も非常に重要な役割を果たします。

IoTデバイスはセンサー、アクチュエータを含んだよりインテリジェントなデバイスが使われると想定されますが、これまで説明してきたように、物理セキュリティ環境の依存性が少ない環境の利用がより進むことも想定されます。現時点でそのような「弱い物理セキュリティ環境」で利用されている代表的なデバイスとしては、交通カードなどのICカードがあげられます。IoTデバイスにおいても、ICカードと同様に物理的攻撃に強い耐タンパーなセキュアエレメントと、そこに格納された暗号鍵やクレデンシャルなどから構成されるIoTデバイス自体のハードウェアセキュリティが非常に大きな意味を持ちます。

4. 車におけるトラストのパラダイムシフト

「物理セキュリティ環境によるトラスト」から、「暗号技術によるトラスト」へパラダイムシフトが起こりつつあるものの一つに自動車があります。

現在の自動車は、排気ガス規制をクリアするためのエンジン制御に始まり、車両姿勢安定化システム、自動ブレーキシステム等、自動車の多くの制御がECU(Electronic Control Unit)により実現されています。そして現在では、自動運転等を巡って熾烈な開発

競争が起きています。また、利用者ニーズに対応するビジネス戦略のようなところでも、いろいろなITサービスと自動車をつなぎたい、利用者のさまざまなITデバイスを自動車につなぎたいといった要求が高まっています。

従来からのECUおよびECUを繋ぐ車載LANは、重要インフラの制御ネットワークと似た性格がありました。すなわち、車載LANは、車内という閉じた物理セキュリティ環境で守られたクローズドネットワークであるという前提で設計され、ECUに関する多くのセキュリティも、設計の秘密で多くが守られてきたところがあります。

こうした状況に対して「つながることにより価値を高める」という要求を満たすために、車の外部的にも、車の内部的にも、デジタルデータの連携やECUの連携による制御の要求が高まっています。こうしたことから、車載LAN、ECUなどの状況が大きく変化しつつあり、それに対応するために、暗号技術によるトラストが求められるようになって来たと言えます。

「暗号技術によるトラスト」の観点から見たECU・車載LANの理想的な実装は、設計の秘密が最小限であり、暗号鍵が格納された耐タンパーなセキュアエレメントが個々のECUに格納されたものになります。そして、自動車がユーザーの手に渡った後でもECU自身が持つセキュアエレメントに格納された信頼の起点（Root of Trust）を元に、様々な外部からアクセス時のアクセス管理・権限管理や、ECU自体のプログラム管理（例えばコード署名の検証）がおこなわれることになります。ECU外部との信頼関係に基づいたアクセス管理では、車載LANを介して他のECU等との信頼関係や、ECUを介した通常時における外部との信頼関係に加えて、車検時や故障時にディーラーでおこなわれるような車およびECUの保守時のアクセス管理も重要になります。

この車およびECUの保守時のアクセス管理の問題は、多くの重要インフラの制御システム等も同様の課題を抱えています。自動車も重要インフラも、利用者および周囲の人間の生命の安全に重大な影響を及ぼす可能性があるため、様々な場所での保守やリモート保守の仕組みが不可欠となります。しかし、このリモート保守回線や保守ポートがサイバーセキュリティ的にはバックドアになっている場合が少なくなく、これが新たなサイバー攻撃の脅威となっています。

こうした課題に対応するECUのセキュリティ要件は、様々なところで議論されています。例えば、欧州の新しいR&DフレームワークHorizon 2020のプロジェクトであるSHARCS (Secure Hardware-Software Architectures for Robust Computing Systems) プロジェクト[4]において取りまとめられた要求があります。表1は、このプロジェクトが2015年12月に公開した報告

表1 自動車の ECU における権限管理

番　号	ロール	権限レベル	権　限
ユーザロール１	ECU 製造者	高い	ECU 自体へのアクセスとアップデート
ユーザロール２	自動車メーカー		各装置へのアクセスとアップデート
ユーザロール３	修理工場		自動車メーカーから配布されたツールをもとに各装置へのアクセスとアップデート
ユーザロール４	検査機関 / 警察		OBD ポートから各装置の状態の読み込み
ユーザロール５	オーナー / 運転手	低い	アクセス権なし

Horizon 2020 Program, SHARCS(Secure Hardware-Software Architectures for Robust Computing Systems), Deliverable D2.1, “SHARCS Applications and framework requirements for secure-by-design systems” から抜粋・訳

書[5]で示されたECUのECU外部からのアクセス権限リストになります。この表からも分かる通り、1台の自動車に非常に多くののECUが搭載される中、その中の1台のECUでさえも数多くのクレデンシャル管理・アクセス権限管理が必要になります。

以上で説明した「物理セキュリティ環境によるトラスト」から「暗号技術によるトラスト」へのパラダイムシフトは、今後、自動車に限らず様々な業界に波及し、それが今後の社会を支えるIoTシステムとなって行くと考えられます。

5. おわりに

本稿では、IoTデバイス、IoTシステムにおける暗号技術によるトラストの重要性を中心に説明してきました。暗号技術によるトラストは、IoTのセキュリティのベースとなるものであると同時に、IoTビジネス、サービスのベースとなるものです。

しかし、そもそもリソースが限られるIoTデバイス等に暗号技術を実装していくのは容易ではありません。IoTデバイスの省電力等の要求や、制御の時間等の要求から軽量な暗号アルゴリズムや軽量な暗号プロトコル、低遅延な暗号アルゴリズム等が必要になる場面も考えられます。IoTサービスの運用面から見た場合の課題は、なんと言っても大量のIoTデバイスに対応する大量の暗号鍵管理（暗号鍵の配置展開）をどのように行うのか等があります。このようにIoTにおける暗号技術は、非常に多くの技術的なチャレンジが必要な分野になります。

紙面の関係等もあり、今回は、暗号技術によるトラストを実現するための技術課題等は十分に説明できませんでしたが、まずは、暗号技術によるトラスト自体の重要性についての理解の助けに多少でもなれば幸いです。

参考資料

[1] 第2回 CRYPTREC の在り方に関する検討グループ　資料
http://www.meti.go.jp/policy/netsecurity/cryptrec_hp02.pdf

[2] データセンター設備のサイバーセキュリティ対策に向けた活動開始～「ファシリティ・インフラWG」をキックオフ
http://www.jdcc.or.jp/news/article.php?nid=eccbc87e4b5ce2fe28308fd9f2a7baf3&sid=108

[3] 建物設備システムリファレンスガイド 第1版、日本データセンター協会＆東大グリーン ICT プロジェクト
（非公開）

[4] SHARCS Secure Hardware-Software Architectures for Robust Computing Systems
http://www.sharcs-project.eu

[5] Deliverable D2.1: SHARCS Applications and framework requirements for secure-by-design systems
http://www.sharcs-project.eu/m/filer_public/39/f7/39f7a59a-c305-412d-9ce0-480df1d2ac50/sharcs-d21.pdf