ハードウェアセキュリティ技術・暗号技術の社会実装における課題

国井 裕樹[1,a)]　伊達 浩行[1]　伊藤 忠彦[1]

概要：IoT 機器の爆発的な普及に伴い, IoT セキュリティ技術はより重要性を増す. しかしながら, セキュリティ技術の根幹となるハードウェアセキュリティ技術・暗号技術の導入については, 進んでいるとはいいがたい現状である. 本稿では, IoT が適用される分野ごとの現状を踏まえた上でユースケースの検討を行い, IoT 機器への暗号技術の導入に向けて, IoT セキュリティの社会実装における課題抽出としてハードウェアセキュリティ技術・暗号技術への実装要件を導出した.

Identifying bottlenecks on social implementation of Hardware Security and Cryptography

Kunii Hiroki[1,a)]　Date Hiroyuki[1]　Ito Tadahiko[1]

Abstract: With the explosive popularization of IoT devices, the security technology of IoT becomes more important. Howerver, it is hard to say that the introduction of hadware security and cryptographic technology which is the foundamental technology of security is progressing at present. In this paper, based on the current state of each field to which IoT is applied, we have considered sevral use cases for the introduction of hardware security and cryptographic technology into IoT device. Through the use cases, we have derived implementation requirements of hardware security and cryptographic technology for IoT devices as the identification of bottlenecks on social implementation of IoT security.

1. IoT 機器におけるセキュリティと暗号技術とトラスト

1.1 背景と課題

IoT が普及した社会における情報システムでは, 大量のセンサが情報を収集し, 膨大なデータはクラウド上のデータセンタに送られ, ビックデータとして蓄積, 処理される. そして, 処理結果に基づき, 社会に対して質が高く快適で便利なサービスが提供される. IoT が注目されている大きな理由として, 前述の世界観が幅広い分野で共有されていることがあげられる.

IoT におけるセキュリティ対策としては一般の ICT におけるセキュリティ対策と同様に多層的に防御することが重要となっているが, 最も根本的で本質的なセキュリティ対策として, ハードウェアセキュリティ技術と暗号技術を利用した対策がある.

しかしながらこれらの対策は, 現状ではコスト等の面からセキュリティは後回しにされることが多々あり, 脆弱な IoT 機器が多数存在している. よって, コストは IoT セキュリティにおける大きな課題であることは間違いない. IoT セキュリティの社会実装が広く行われるためには, システム全体の堅牢性・信頼性・可用性を効果的に確保した上で, 「つながる」ことでコストを上回る新しい価値が生まれるような将来の IoT システムのモデルを検討する必要がある.

1.2 研究のアプローチ

本稿では, 技術的な視点としてハードウェアセキュリティおよび暗号技術に着目する. これらはセキュリティの根本をなすものであるが, 同時にシステム全体の信頼に関わる重要な技術でもある. 信頼を構成する重要な概念とし

[1] セコム株式会社 IS 研究所
〒 181–8528 東京都三鷹市下連雀 8–10–16 セコム SC センター
[a)] h-kuni@secom.co.jp

て「トラスト」がある。ここでは, コミュニケーションの相手, 情報, システムなどが正しいと判断できる状態にあることを「トラスト」と定義する. 「トラスト」は IoT システムに限らず情報システム全般において重要である. 言葉だけを聞くと当然の内容であり, 特別重要な概念であるとは捉えられないかもしれない. しかし, 開発, 販売, 運用, 廃棄といったライフサイクル全体で関わってくる全てのステークホルダについて, コミュニケーションの相手, 情報, システムが正しいと判断できる状態にすることは非常に難しい. 寿命が数日である機器はもちろんのこと, 数十年も利用する機器に対しても, 開発時の設計段階でライフサイクル全体の「トラスト」をどう構築するかデザインしなければならない. また, 機器の製造に携わる人手の数が多ければ多いほど, そのステークホルダ間での「トラスト」の構築は複雑なものとなる. 機器を取り巻く環境は移ろい行くものであり, 設計の前提となるもの, ステークホルダ間の関係性などは様々に変化していく. このように安定性を継続できる要素が少なく予想も難しい中で, どこかに「トラスト」構築の不備があれば, そこをついた不正な行為を許すこととなる. 当然, ライフサイクル全体の「トラスト」を構築するためには他の技術も必要となるが, 正しさを保証するという点において, 理論や研究に裏打ちされた堅牢性を備え, 一定の安定性を継続できる暗号技術は非常に有用である. 暗号化での情報・通信の秘匿, 認証によるコミュニケーション相手の確認, 電子署名によるデータ改ざん検知など, 暗号技術なしには容易に達成しえない技術は多くあり, この暗号技術の中心となる暗号鍵の管理においてハードウェアセキュリティが最終的な信頼の基点となり「トラスト」を実現する.

本稿では, IoT システムにおける本来の価値を最大化する技術としてのハードウェアセキュリティと暗号技術が, どのようなシステムやサービスで社会実装されうるのか, そこにどのような要件が必要なのかを調査・検討する. ハードウェアセキュリティの重要な利用方法として暗号鍵管理での利用を挙げたが, 調査に当たってはそもそも暗号技術が利用されるか否かを調査・分析した上で, その分野においてハードウェアセキュリティは暗号鍵管理に利用されるべきであるという考えである. すなわち, ここではハードウェアセキュリティは暗号技術が組み込まれる際の鍵管理に利用されることを前提とする. 複数のメーカーから調達された機器で構成されるシステムを運用し, 他システムと相互接続されることが見込まれる, 又は人命等の重要資産にクリティカルな影響を与える事が想定される分野, かつ今後より強固なセキュリティを確保するために IoT 機器へハードウェアセキュリティと暗号技術を組み込むことが必須と考えられる分野という観点で以下の 4 つの分野を選定した.

- 防犯カメラシステム
- ビル管理システム・データセンタ
- 自動車
- ヘルスケア機器

本節以降では, 2 節で各分野における既存または検討中の暗号技術を用いたセキュリティ対策やセキュリティへの要求が業界標準に存在するか, または現在検討されている標準規格における暗号技術を用いたセキュリティ対策の有無を述べる. 3 節では, IoT システムにおいて全体の堅牢性・信頼性・可用性を効果的に確保でき, 「つながる」ことで新しい価値が生まれるような暗号技術を用いたユースケースを検討する. 4 節では, 3 節で上げたユースケースに対して, IoT セキュリティの社会実装の課題抽出として IoT 機器の暗号技術, そしてその暗号鍵を守るためのハードウェアセキュリティの実装要件を検討する.

2. 標準規格・ガイドライン調査

2.1 防犯カメラシステム

本節では, 国内外の団体が発行する防犯カメラシステムの各ガイドラインでのセキュリティに関する記述の概要を述べる.

2.1.1 ONVIF によるガイドライン

ONVIF（Open Network Video Interface Forum）は, IP で通信を行う防犯カメラに代表されるフィジカルセキュリティ製品に関する国際的なフォーラムである, ONVIF では, コア部分に関する標準仕様 [1] にセキュリティに関して, TLS を利用するための記述がなされている.

2.1.2 PSIA によるガイドライン

PSIA(Physical Security Interoperability Alliance) は, 国際的なフィジカルセキュリティ製品やサービスに関する国際的な団体である. PSIA ではデータに関するアクセス制御等に関しては詳しく記述しているが, 直接的なセキュリティに関する記述は少なく, TLS1.0 以上の利用を求めている（同ガイドライン 6 節）.

2.1.3 BSI によるガイドライン

BSI(British Standard Institute) による防犯カメラシステムに関するドキュメント [2] においてセキュリティに関連する記述の多くは”System Security”(システムのセキュリティ) に関する記述であり, ”System Integrity”（システムの完全性）と”Data Integrity”（データの完全性）に関しての注意点等が詳しく記載されている.

2.2 ビル管理システム/データセンタ

本節では, ビル管理システム分野およびデータセンタ分野における, 標準通信プロトコルやガイドラインについての調査結果をまとめる.

2.2.1 BACnet

BACnet はビル管理システムとして国内外で広く利用されている BACnet（A Data Communication Protocol for

Building Automation and Control Networks）は, 複数のベンダから提供されるビルディングオートメーション用機器を相互接続するための通信プロトコルであり, ISO 16484-5:2017[3] として標準化されている. セキュリティに関する記述としてはメッセージの認証, 秘匿の方式を規定している（同規格 24 章）. 末端機器でメッセージの認証処理, 秘匿処理を行うことに加えて, BACnet のセキュリティ機能に対応したシステムと未対応のシステムとの接続のために, ネットワーク機器でメッセージ認証や認証データの付与/削除, 暗号化/復号を行う方式も言及されている.

2.2.2 LonWorks

LonWorks（Local Operating Networks）は, 米国エシェロン社が開発した, ビルオートメーションや制御ネットワーク向けの通信技術である. LonWorks の通信プロトコルには, ISO/IEC 14908-1[4] として標準化されている LonTalk[5] を使用する. LonTalk でのセキュリティに関する記述としては, メッセージ認証（同規格 9.11 節）と秘匿（同規格 9.12 節）の方式を規定している.

2.2.3 建物設備システム リファレンスガイド

建物設備システムリファレンスガイド [11] は, 特定非営利活動法人日本データセンター協会が, データセンターの建物設備システムとそれを監視制御するビルオートメーションシステムのあり方や, 設計, 調達, 運用の各段階での注意点をまとめたものである. 建物設備システムの将来あるべき姿として「M2M/IoT 時代の建物設備システム」について触れており, 具体的な方式に関する記述はないものの, 「ネットワーク単位でのアクセス制御が事実上不可能となることを前提にしたシステム設計と構築が必要となります. 一例としては, 個々のデバイスが個別に認証をおこない, セキュアな通信経路を確保する構成が考えられます.」とある.

2.3 自動車

本節では自動車分野における標準規格についての調査結果をまとめる.

2.3.1 IEEE1609.2

IEEE1609 は, 5.9GHz の DSRC 向け Wireless Access in Vehicular Environments(WAVE) として, 主に車車間通信 (V2V) や路車間通信等 (V2I) を対象として IEEE で策定されている無線通信の標準規格群である. その中の 1 つである 1609.2 は, セキュリティ部分をスコープとしてメッセージフォーマットやその処理について定義をしている. IEEE1609.2-2016[12] では暗号技術を使ったセキュリティに対する詳細な言及があり, 楕円曲線暗号が認証・署名等の用途で指定されている.

2.3.2 ITU-T X.1373

ITU-T X.1373[14] は, ITS(Intelligent Transportation System) などに必要とされている車載器ソフトウェアの無線でのアップデートにおけるセキュリティを規定した標準規格である. 2017 年に Recommendation として ITU-T から発行された. セキュリティに関する記述としてはアップデートにおける通信メッセージの検証方式として, 電子署名の検証や MAC(Message Authentication Code) による検証方式を一例としてあげているほか, 通信の秘匿化については TLS など通信レイヤーでの実装を考慮している.

2.3.3 EVITA

EVITA(E-safety vehicle intrusion protected applications) は, 欧州において 2008 年から 2011 年まで FP7 のプロジェクトとして, 自動車の情報システムと利用手順の整理から特定の利用環境に応じた脅威分析を行ったうえで, 情報セキュリティ対策を検討していた. 2011 年に発行された Deliverable D3.2[15] では, 車車間通信や路車間通信等 (V2X) に必要とされる暗号技術を含めたセキュリティ機能を搭載したハードウェアの機能セットを定義している.

2.4 ヘルスケア機器

本節では, ヘルスケア機器分野における標準通信プロトコルやガイドライン, 法律についての調査結果をまとめる.

2.4.1 DICOM

DICOM（Digital Imaging and COmmunications in Medicine）は, CT や MRI などの医療用画像データを異なるベンダの機器やシステム間で交換するための標準規格として NEMA(National Electrical Manufacturers Association) により管理され, ISO 12052:2017[18] で標準化されている. セキュリティに関する記述としては, ネットワークセキュリティに関して [19], 例えば, DIMSE(DICOM Message Service Element) プロトコルでデータを送信する際に TLS を利用する機器やシステムは, 「The Basic TLS Secure Transport Connection Profile」や「The AES TLS Secure Transport Connection Profile」をサポートする必要があるという記述がある.

2.4.2 医療情報システムの安全管理に関するガイドライン

医療情報システムの安全管理に関するガイドライン [20] は, 厚生労働省が, 医療情報の電子的な取り扱いについて, 技術的および運用管理上の注意点をまとめたものである. 診療録等が機微な個人情報であることから, 医療情報システムの安全管理に関するガイドラインには, セキュリティに関する要求事項も数多く記載されている. 情報漏えいを防止するためのデータや通信経路の暗号化, データの改ざんを検知するための電子署名, 通信先を適切に識別するための認証, の必要性について記述されており, SSL/TLS, IPsec, S/MIME などの技術が例示されている.

2.4.3 IHE

IHE(Integrating the Healthcare Enterprise) は, 医療情報システムの相互互換性を推進するプロジェクトである. セキュリティに関する記述としては,「Audit Trail and Node

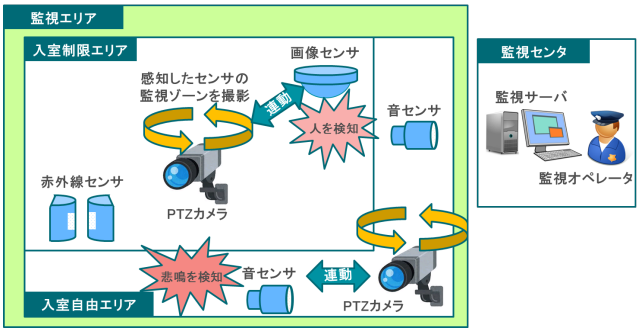
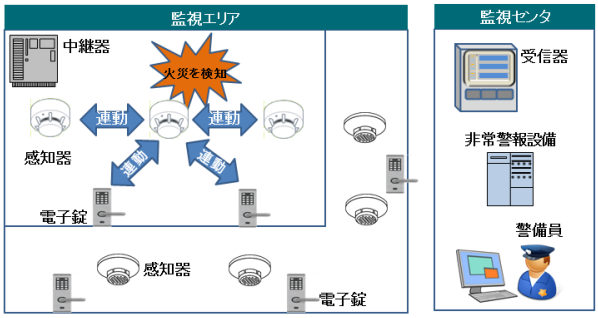


図 1　防犯カメラシステム



- 連動機能により、付近の感知器の感度を上げ、電子錠を解錠する。

図 2　IoT 自動火災報知システムの連動機能

Authentication」統合プロファイル [21] 中の「Authenticate Node」トランザクション [22] において, 電子証明書による認証について記述がある. また, TLS の利用や S/MIME の利用に関する記述もある.

3.　ユースケース

2 節で, 各分野において暗号技術を用いたセキュリティ対策への要求が存在していることは明確になった. 本節では暗号技術の導入に向けて, IoT システムにおいて全体の堅牢性・信頼性・可用性を効果的に確保でき, 暗号技術を用いセキュリティ技術を使って「つながる」ことで新しい価値が生まれるようなユースケースを検討する.

3.1　防犯カメラシステム

ここでは, 不特定多数の人が通る公開された空間 *2 が含まれる施設に設置された防犯カメラを想定し, 各防犯カメラが広域網を通じて管理システムに接続するオンライン防犯カメラシステムを例としてユースケースを検討する.

本節では, 図 1 記載の防犯カメラシステムを想定する. この防犯カメラシステムにおいては, PTZ カメラと多数のセンサが連動し, 監視エリアを監視するものとする.

高精細な画像を用いて 1 台のカメラで広い領域を監視するために, 一般に PTZ カメラ（パン・チルト・ズーム機能を持つ）が用いられている. しかし, PTZ カメラは, 高価であり, 設置コストも高く, 1 台のカメラのみでカバーできる範囲にも限界がある. そこで, コストを抑えて詳細な画像監視を行う為に, 安価なセンサ（空間センサや固定カメラ）を PTZ カメラと併用した防犯カメラシステムが図 1 となる.

こうした防犯カメラシステムは単独のカメラを複数付ける従来型のシステムに対し, コスト面でのメリットは大きい. 一方で, 当然つながることによるセキュリティへの懸念が存在し, 防犯のためのシステムとして堅牢性・信頼性・可用性は確実に確保されるべきである.

*2　通行人に対し, 物理的なアクセス制御が為されていない空間.

3.2　ビル管理システム/データセンタ

ここでは, IoT 機器として火災センサに着目し, 火災の発生をより正確に検知できる自動火災検知システムを検討する. このシステムは従来の接点入出力ではなく, LAN 等のデジタル通信で各機器が接続される自動火災報知設備（以降, 「IoT 自動火災報知システム」とする）を検討する.

IoT 自動火災報知システムでは, ある感知器が火災, または火災の可能性を検知した場合, 最初に火災を検知した感知器とその周辺の感知器が感度を上げる. そして, システムが火災発生と判断した場合には, 避難経路上の扉に設置された電子錠の解錠制御を行う（図 2）.

通常, このような連動は, ある区画毎に設置される中継器や, 監視センタに設置されている受信機を介して行われるが, 感知器から中継器への通信が行えない場合は, 感知器は周辺の感知器や電子錠に直接信号を送信する.

また, 中継器は, 定期的に感知器の死活監視を行い, 感知器が正常に機能していないと判断した場合には, 受信機にその旨を通知すると共に, 周辺の感知器の感度を上げるように制御する. このように各機器が連携することで, IoT 自動火災報知システムは, より信頼性の高い自動火災報知設備となり得る. 設置コストの観点から感知器への有線の引き込みが不要となるように, 感知器は無線通信に対応した電池駆動のものを想定する.

こうした自動火災報知システムは従来型のシステムに対し, コスト面でのメリットは大きく, また信頼性・可用性の面においても向上が見込める. 一方で, 当然つながることによるセキュリティへの懸念が存在し, 向上した信頼性・可用性は防災システムとして確実に確保されるべきである.

3.3　自動車

ここでは, 自動車と様々なものが通信を行う V2X(Vehicle to X) におけるユースケースを検討する.

自動車分野では V2X と言われる自動車と様々なモノが通信を行うための議論が進んでおり, ETC や ITS(Intelligent Transport Systems), テレマティクスと呼ばれるサービス

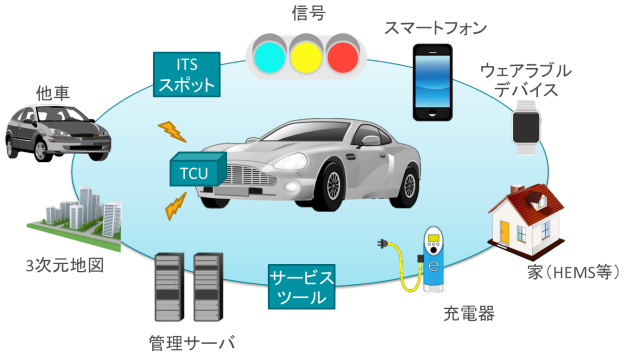


図 3　V2X におけるユースケース

から, さらに拡張される方向に業界として向かっている. これらは IoT のユースケースとしてはいち早く取り入れられている事例であり, 今後も様々な方法で自動車がつながる「コネクテッドカー」の時代がやってくると考えられている. 以下で将来的なコネクテッドカーのユースケースを列挙する.

自動運転時代を見据え, 自動車は他車との通信および路側機等のインフラと通信を行い, 協調型の制御を行う. また 3 次元地図もネットワークから自動車内に取り込み周辺の状況を取得する. 利用者が持つスマートフォンやウェアラブルデバイスの情報を用いて個人の嗜好に合わせた設定や体調の変化を察知し, 家や充電器との接続において各種の情報を提供する.

こうした V2X におけるシステムは, 自動運転の動きから見ても将来実現される可能性が高い. 一方で, 当然つながることによるセキュリティへの懸念が存在し, 人命に直結する場面も多いため, 堅牢性・信頼性・可用性が確実に確保される必要がある.

3.4　ヘルスケア機器

ここでは, 同一機器で複数のサービスを利用できるヘルスケア用ウェアラブル機器を検討する.

利用者が, デザイン, 機能, 使いやすさなどに基づき, 自身の利用したいウェアラブル機器と健康管理サービスとを自由に組み合わせて利用できるヘルスケアサービスを提案する. このようなサービス形態が可能になると, 利用者の満足度を高められ, ヘルスケアサービスの市場拡大につながるとともに, 機器ベンダやサービス事業者は, それぞれが自身の得意分野に注力してビジネスを展開できる.

もし, ウェアラブル機器とサービスとを自由に組み合わせて利用できると, 利用者は, 1 つのウェアラブル機器から複数の健康管理サービスを利用したいと考えるかもしれない. さらに, ウェアラブル機器から自動車へデータを送信することで「睡眠時間が不足しているので, 運転開始時に注意喚起する」など, 新たな連携によるサービス提供の可能性も高まる（図 4）.

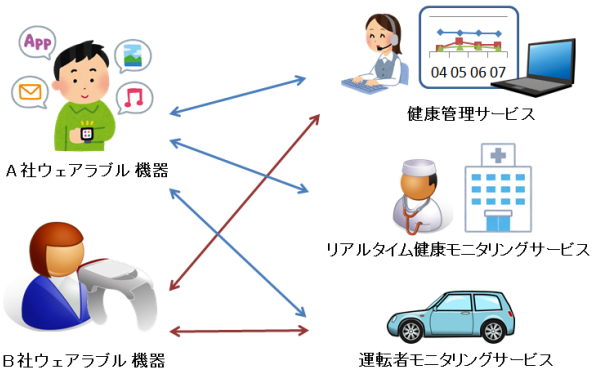


図 4　将来のヘルスケアサービス：同一機器で複数サービスを利用する場合

こうしたヘルスケア用ウェアラブル機器を使ったシステムは, ユーザーが自身の情報を複数システムで利用することによる直接的なメリットを享受しやすい. 一方で, 当然つながることによるセキュリティへの懸念が存在し, 機微情報とされるバイタル情報を扱うため, 堅牢性・信頼性は確実に確保されるべきである.

4.　IoT 機器への暗号技術の実装要件

本節では 3 節であげたユースケースをもとに, IoT 機器へのセキュリティ技術における暗号技術の導入にフォーカスして, その実装要件を検討する.

今回はシステム開発およびシステム運用での有効性を念頭に以下の条件で検討を行う.

- 実装コスト
- 運用コスト
- スケーラビリティ

以上の条件とユースケースであげた事例をもとに, IoT システムにおける本来の価値を最大化するために必要なセキュリティ技術としての暗号技術の実装要件を検討する. 暗号技術の実装コスト削減, 導入による運用コストの低減, 普及時におけるスケーラビリティの確保といった観点で以下の 4 つの実装要件を抽出した. 各項目ごとに詳細を記述する.

(1) 公開鍵暗号の利用

暗号方式には大きく分けて共通鍵暗号と公開鍵暗号の 2 種類がある. 実装コストや処理性能を考えると共通鍵暗号に利があるが, IoT 機器の普及数とユースケースの前提となるマルチステークホルダでのセキュリティの実現を考慮すると共通鍵暗号を用いたセキュリティでは数が増大するにつれ鍵管理コストが課題になる. マルチステークホルダ間での鍵共有においては PKI(Public Key Infrastructure) の利用も期待されることから, 公開鍵暗号を用いる方式を採用できること

が求められる.

(2) 軽量性（省電力性）

IoT 機器は多様であり, リソース面においても豊富なものから限られているものまで広く存在する. 特にリソース (例えば計算処理, メモリ消費, バッテリー消費) が限られた機器では, セキュリティが本来の目的の処理に影響を与えてはならない. 3 節のユースケース内でも電池で動くデバイスの利用が想定されているが, それらの用途では省電力性は非常に重要な価値となる. 運用コスト面・スケーラビリティから考えても電池交換のコストを下げることは大きなメリットとなるため, 利用される暗号技術には軽量性 (計算・メモリ量) が求められる.

(3) 高速性

ユースケースにある通り, 自動車やセンサといった IoT 機器は多数が通信しあって, その価値を増大させる. このときセキュリティを確保するための仕組みがボトルネックになることが課題となることが多々ある. 暗号技術も同様の課題をもっており, メッセージの正当性を証明する情報を付加する場合, 1 つのノードに大量に通信が流れ込むと検証処理がボトルネックになることが想定される. この場合にはスケーラビリティの観点から検証処理をなるべく高速化し, 効率的にメッセージを処理する必要がある.

(4) 物理攻撃への耐性

IoT 機器で暗号技術を用いる場合には, 機器のライフサイクル全般に渡って暗号鍵が正しく管理されなければならない. 特にコンシューマ向けの IoT 機器においては, 機器の入手性は高く, 攻撃者の手に渡る可能性もあり, 暗号鍵を守るための耐タンパ性は確実に求められる. ハードウェアセキュリティの実装要件はまさにこれにあたる. またサプライチェーン全般での対策も必要であり, 製造・流通行程における攻撃への対策も必要とされる.

5. おわりに

本稿では IoT システムにおける本来の価値を最大化するために必要なセキュリティ技術としての暗号技術が, どのようなシステムやサービスで社会実装されうるのか, そこにどのような要件が必要なのかを調査・検討をし, 4 つの要件を示した.

なお, 本稿の研究は, 総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム (SIP)「重要インフラ等におけるサイバーセキュリティの確保」(管理法人:NEDO) によって実施されたものである.

参考文献

[1] ONVIF Core Specification version 2.6.1, December 2015.
[2] BS EN 62676-1-1:2014,Video surveillance systems for use in security applications. System requirements. General.
[3] ISO 16484-5:Building automation and control systems (BACS) – Part 5:Data communication protocol.
[4] ISO/IEC 14908-1: Information technology – Control network protocol – Part 1: Protocol stack.
[5] Echelon Corporation, "LonTalk Protocol Specification Version 3.0", 1994.
[6] ECHONET CONSORTIUM, "The ECHONET Specification Version 3.21", 2005.
[7] ISO/IEC14543-4-1:Information technology – Home electronic system (HES) architecture – Part 4-1:Communication layers – Application layer for network enhanced control devices of HES Class 1.
[8] ISO/IEC14543-4-2:Information technology – Home electronic system (HES) architecture – Part 4-2:Communication layers – Transport, network and general parts of data link layer for network enhanced control devices of HES Class 1.
[9] ECHONET CONSORTIUM,"The ECHONET Lite Specification Version 1.12", 2015.
[10] ISO/IEC14543-4-3:Information technology – Home Electronic Systems (HES) architecture – Part 4-3:Application layer interface to lower communications layers for network enhanced control devices of HES Class 1.
[11] 特定非営利活動法人日本データセンター協会, "建物設備システムリファレンスガイド", 2015.
[12] IEEE1609.2:2016 IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, 2016.
[13] 総務省 情報セキュリティアドバイザリーボード ITS ワーキンググループ,
[14] ITU-T X.1373:2017 Secure applications and services - Intelligent transportation system (ITS) security, Secure software update capability for intelligent transportation system communication devices, 2017.
[15] EVITA, "D3.2 Secure on-board architecture specification", 2011.
[16] Connected Car 社会の実現に向けた研究会, "Connected Car 社会の実現に向けて（取りまとめ素案）", 2017.
[17] 総務省, "次世代 ITS の実現に向けて", 2015.
[18] ISO 12052:Health informatics – Digital imaging and communication in medicine (DICOM) including workflow and data management.
[19] DICOM PS3.15 2017c - Security and System Management Profiles, National Electrical Manufacturers Association, 2017.
[20] 厚生労働省, "医療情報システムの安全管理に関するガイドライン第 5 版", 2017.
[21] IHE IT Infrastructure(ITI) Technical Framework Volume 1 (ITI TF-1) Integration Profiles, 2017
[22] IHE IT Infrastructure Technical Framework Volume 2a (ITI TF-2a) Transactions Part A - Section3.1-3.28, 2017
[23] Manufacturer Disclosure Statement for Medical Device Security, National Electrical Manufacturers Association, 2013.