IoTデバイスに対するDoS攻撃が出力信号に与える影響と対策に関する研究

神内 良太[1,a)]　猪俣 敦夫[2,1]　新井 イスマイル[3]　藤川 和利[3]

概要：近年 IoT の普及により様々なデバイスがインターネットと接点を持ち始めている．そのため攻撃からモノを守るためのセキュリティ対策の確立が急がれているが，IoT に利用される機器は，従来の通信システムと比較して性能や運用方法に大きな違いがあり，これまでの方法では対処できない問題が発生している．特に，対象によってはデータよりもデバイスの安定性が重視される場合も想定されるため，新しい観点からの対策が必要だと考えられる。本稿では外部から行われる可能性のある脅威のなかでも，特に DoS 攻撃のようなデバイスの処理に影響を与える攻撃による負荷測定を行い，出力信号に与える結果を報告し，その原因と対策方法を議論する．

キーワード：システムセキュリティ，ハードウェア，組込みシステム，制御システム

A study of impacts and countermeasures in output signals from IoT devices under DoS attack

Ryota Jinnai[1,a)]　Atsuo Inomata[2,1]　Ismail Arai[3]　Kazutoshi Fujikawa[3]

Abstract: Recently, various devices begin to connect the Internet owing to the spread of IoT(Internet of Things). Therefore it has become an urgent matter to establish new security countermeasures. But IoT device is not able to deal with some new incidents because of difference in performance or operation between IoT and conventional ICT systems. In some cases, stability of IoT device is more important than using data. Therefore we should consider the necessary from new viewpoint of security. In this paper, we show the result of load test and impact on output signals under DoS attack, and we discuss countermeasures and cause.

Keywords: system security, hardware, embedded system, control system

1. はじめに

近年，IoT(Internet of Things) 技術の普及に伴い様々なモノが外部との接点を持ち始めており，インターネットに接続されるデバイス数は爆発的に増加している．調査団体により数に大きく差があるものの，2020 年までには少なくとも 200 億個以上のデバイスがインターネットに接続される見積もられている [1]．その中でも産業分野においては IoT 技術を取り入れ産業システムのさらなる高度化・効率化を目指す試みが世界各国で行われており，特にドイツでは政府主体となって Industrie4.0 というプロジェクトが進められており注目を集めている [2]．我が国においても IoT が産業・就業機構へ与える影響と対応について検討が進められており，日独間で IoT/インダストリー 4.0 協力に関する共同声明を行うなど早急な対策法の確立に向けて本格的に動き始めている [3], [4]．

その一方従来インターネットから切り離されて運用され

1 奈良先端科学技術大学院大学情報科学研究科
Graduate School of Information Science, Nara Institute of Science and Technology
2 東京電機大学
Tokyo Denki University
3 奈良先端科学技術大学院大学総合情報基盤センター
Information Initiative Center, Nara Institute of Science and Technology
a) jinnai.ryota.jl9@is.naist.jp

てきた機器が接続されたことで，外部からの攻撃の危険性が増大しておりその対策が急務となっている．しかし IoT で利用される機器は，従来の通信システムで使用されてきた汎用性の高いコンピュータなどと比較してデバイスの性能や運用方法，攻撃が成功した場合の被害規模などに大きな違いがあり従来のセキュリティ技術をそのまま適応できないケースが多く問題となっている．特に産業分野で用いられる制御システムなどの場合，その特性上被害が甚大なものとなりやすく，昨年の１２月にウクライナで発生した発電施設に対するサイバー攻撃では数時間にわたり停電が発生し国民生活に大きな影響を与えている [5]．またこの攻撃で用いられたとみられるマルウェアの中に日本語の文字列が発見されており [6] 今後我が国も標的にされる可能性が高まっていると考えられる．

本稿では，まず関連研究としてこれまで制御システム向けに研究されてきたセキュリティ技術の一部を紹介し，それらの特徴及び先行研究では考察されていないハードウェアレベルのセキュリティ問題点について検討を行う．その後，IoT 向けのデバイスとして広く用いられている Arduino UNO と mbed LPC1768 に対してデバイスの処理系に負荷をかけることを目的として DoS(Denial of Service) 攻撃を行い，出力信号に与える結果についての検討を行い報告するとともにシステムに与える影響を議論する．

本稿の構成は以下のとおりである．第 2 章では，これまで研究されてきた制御システム向けのセキュリティ技術を紹介するとともにその問題点を指摘し，本研究のモチベーションの解説を行う．第 3 章では実験の目的と使用する機器の説明及びその手法について解説を行い，結果について報告を行う．第 4 章では得られた結果から出力信号を安定化させるための要素について考察を行うとともに今後の課題について述べる．最後の第 5 章で本稿のまとめを行う．

2. 関連研究

本章では制御システムのセキュリティに関する関連研究を紹介するとともに，その問題点について検討を行う．

2.1 制御システムのセキュリティ

情報システムと制御システムのセキュリティにおける簡単な比較を文献 [7], [8], [9] を参考にまとめたものを**表 1** に示す．

その中でも制御システムにおけるセキュリティを考える上で，Alvaro ら [8] は従来の通信システムと大きく異なり問題となる点として以下を挙げている．

- システムをすぐに停止させることができないため，直ちにパッチを当てたりアップデートすることができない．
- 厳密なリアルタイム性が要求される．
- レガシーなシステムのまま使い続けられるものが多い．

表 1 制御システムと通信システムのセキュリティにおける比較

	制御システム	情報システム
優先事項	システムの可用性	情報の機密性
セキュリティの対象	モノ (設備，製品)	情報
システムの更新	10-20 年	3-5 年
連続稼働時間	常に連続稼働	一般には業務時間内
処理制約	厳密なリアルタイム	遅延はある程度許容可能
使用プロトコル	限定的	多岐にわたる
ネットワーク構成	比較的単純	複雑

- 機器の入れ替えが少なく，使用プロトコルも限定されるためネットワークの構成が単純になりやすい．

これらの問題の解決策の 1 つとして，田村ら [10] はシステムを停止することなフォレンジックを行うライブフォレンジックの制御システムへの適応を提案している．またネットワークの構成が単純になるという特徴を生かして，従来のホワイトリスト方式を改良したフローホワイトリストを用いてセキュリティの向上を目指す研究が Rafael ら [11] によって行われており一定の成果を得ている．また産業界においては極力コストの増加を避ける必要があるため，端末での処理能力も低く抑えコストの削減を目指す傾向がある．そのため，従来の方式では低スペックのデバイスにも低コストでセキュリティ対策を行う方法についても問題となっている．この問題に対するアプローチとしては，従来の情報システムで用いられてきた暗号プロトコルを改良する方法と，組込みデバイス向けの軽量暗号技術の開発を目指す方法が盛んに研究されており，後者の一例として Mouha ら [12] によって提案されたメッセージ認証符号の Chaskey などがあげられる．

2.2 既存研究の問題点

これまでの研究は主に従来の情報システムで培われてきたセキュリティ技術を制御システムに合わせた形に改良することでセキュリティを高めることを目的としている．すなわちネットワーク内の機器間でやり取りされる情報自体に重点を置いている場合が多い．しかし表 1 でも示した通り，制御システムにおいては使用されているシステム自体の可用性を重視していることが多い．特に産業システムや重要インフラで用いている制御システムの場合，そこでやり取りされる情報と同等以上にデバイス自体の安定性が重要になる場合も想定される．例えば，建設機械や工作機械が攻撃により本来意図しない誤動作が発生した場合，人体や財産に損害を与える可能性が高い．そこで攻撃下におけるデバイスの安定性・確実性を担保することが今後重要になると考えられる．

仮に攻撃により，やり取りされる情報自体に影響を与えることができなくでも，特定のデバイスから出力されている制御信号に何かしらの問題が発生した場合，通常では想定されていない誤動作が発生するなどシステム全体に悪影響を及ぼす可能性も想定される．次章では，本仮説を検証

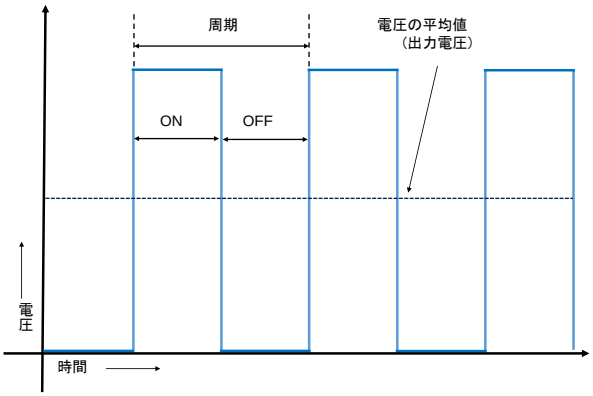

図 1　PWM 制御方式

するために IoT で使用されているデバイスに対して負荷を与える攻撃を行い，出力信号を観測することによってその影響を確認し，システムに与える問題について検証する．

本稿では攻撃の制御システムに与える影響を確認するためにデバイスから出力されている PWM 信号に注目した．PWM 信号は制御性と効率性が高く広く使われている技術の一つであり，制御システムでも重要になると考え今回の観測対象に選んだ．

3.　検証実験

本章では前章で述べた仮説の検証実験の結果について報告するとともに，その影響がシステム全体に脅威を与える可能性について検討を行う．

3.1　PWM

検証実験ではデバイスからの出力される PWM 信号を観測対象とする．PWM(Pulse Width Modulation) とは電圧制御方式のひとつで，特に直流モータのチョッパ制御で最も採用されている制御方式である [13]．PWM 方式では，一定周期中のパルス波の ON/OFF の比率を変化させることで出力される電圧の制御を行う (**図 1**)．チョッパ制御のスイッチの ON/OFF を切り替える時間をスイッチング周期と呼ぶ．また，スイッチング周期中の ON/OFF の比率をデューティ比と呼び，デューティ比が大きいほどパルスの幅が広くなり，出力される電圧の平均値が高くなる．汎用性の高さから，組込み用デバイスには PWM 出力用の Output ピンを搭載し容易に利用ができるように設計されているものも多い．

3.2　実験環境

表 2 に示す 2 種類のデバイスに対して実験を行う．今回用いた ArduinoUNO と mbed LPC1768 は IoT 用途で用いられるデバイスの中でも特に普及が進んでおり，その拡張性の高さから今後も様々な分野で活用されることが見込まれるため今回対象に選定した．本実験では各デバイスは独立したネットワーク内で攻撃用端末と接続されている．通信プロトコルとしては一般の通信システムに使用されている TCP/IP を使用する．Arduino Uno には Ethernet コントローラとして W5500 を搭載したイーサネットシールド 2 を用い，mbed LPC1768 には本体の Ethernet ピンに RJ45 コネクタを接続することで，Ethernet 接続による通信を可能にしている．各デバイスは出力信号の制御機器としての機能と簡易なウェブサーバとしての機能を持っており，外部と HTTP 通信を行うことが可能となっている．今回の実験では DoS 攻撃の種類として情報システムで広く観測されている SYN Flood 攻撃と HTTP GET Flood 攻撃を選んだ．SYN Flood 攻撃には Metasploit Framework に収録されているツールを使用し，5 分間 SYN パケットを送り続けた．HTTP GET Flood 攻撃には Apache JMeter を使用し，スレッド数 20，Ramp-Up 期間 100 秒，ループ回数を無限として 5 分間 HTTP GET リクエストのパケットを送り続けた．また，PWM の周期は両デバイスとも 20ms とし，信号の観測はオシロスコープを用いた．

表 2　使用デバイスの性能比較

device name	processor	performance
Arduino Uno	ATmega328	clock: 16MHz RAM: 2KB ROM: 32KB(Flash) +1KB(EEPROM)
mbed LPC1768	Cortex-M3	clock: 96MHz RAM: 32KB ROM: 512KB(Flash)

3.3　結果

3.3.1　Arduino Uno について

PWM 信号のパルス波の切り替え点における通常時の信号の波形の軌跡を**図 2** に，SYN Flood 攻撃下における出力信号の波形の軌跡を**図 3** に，HTTP GET Flood 攻撃下における出力信号の波形の軌跡を**図 4** にそれぞれ示す．観測はオシロスコープの残光表示を用いて行い，観測時間は 5 分間とした．

攻撃下においては出力信号のパルス幅が目標値以上になる頻度が増加していることが確認できた．また SYN Flood 攻撃と HTTP GET Flood 攻撃を比較した場合，HTTP GET Flood 攻撃のほうが出力信号に影響を与えていることが確認できる．逆に SYN Flood 攻撃では通常時に発生する信号のノイズと比較して発生頻度に差がみられるもののパルス波の最大幅にはほとんど変化が見られない．この差の原因の一つとしては，本実験で使用している Arduino Uno では TCP/IP 通信に係る処理を主にイーサネットシー

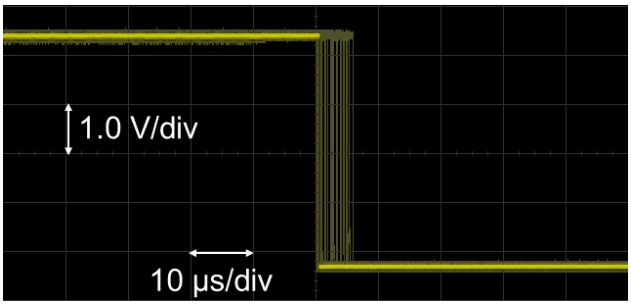

図 2　通常時の波形の軌跡 (Arduino UNO)

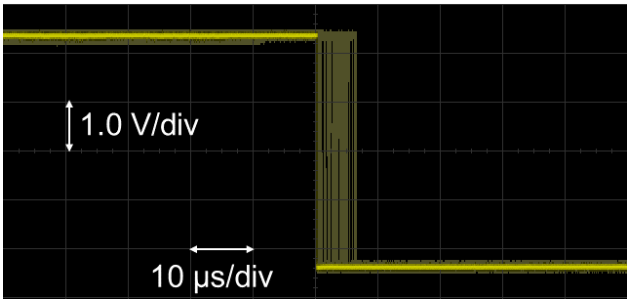

図 3　SYN Flood 攻撃下の波形の軌跡 (Arduino UNO)

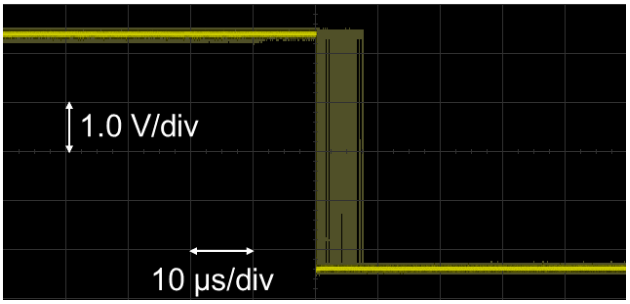

図 4　HTTP GET Flood 攻撃下の波形の軌跡 (Arduino UNO)

ルド 2 に搭載されている W5500 で行っていた点があげられる．TCP の機能を悪用した SYN Flood 攻撃では攻撃による処理の大半は W5500 に向けられたため，出力信号を処理している Arduino Uno 本体にそれほど負荷をかけることができなかったと考えられる．

パルス波の幅の目標値との誤差は，通常時で最大約 6μs 分，SYN Flood 攻撃下では約 6.5μs 分とほとんど差がなかった．しかし，HTTP GET Flood 攻撃下においては目標値と比較して最大約 8μs 分の誤差が生じており，その発生頻度も他の状態と比較して高い．PWM 制御では目標電圧に応じてパルス波の幅を調整しているため，パルス波の幅に高い確立で誤差が生じることは，制御対象に出力される制御信号が本来の意図とは異なった値となってしまう危険性が高くなると考えられる．そのため，制御対象となるモータ等の種類によっては回転速度などに影響を与える可能性があると推測される．

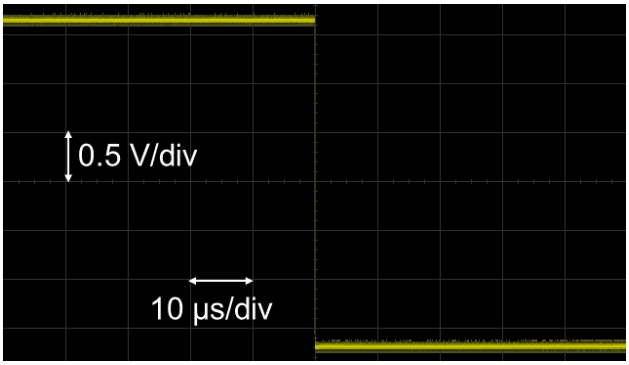

図 5　通常時の波形軌跡 (mbed LPC1768)

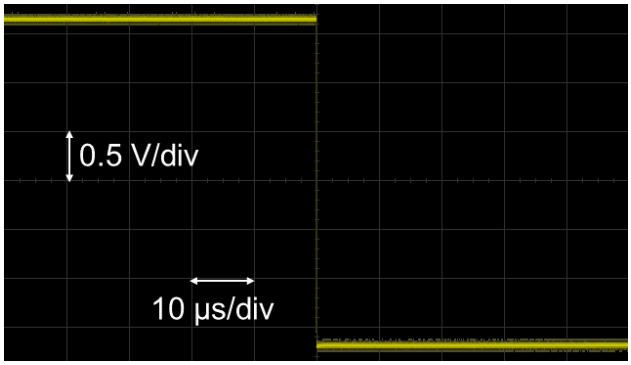

図 6　SYN Flood 攻撃下の波形の軌跡 (mbed LPC1768)

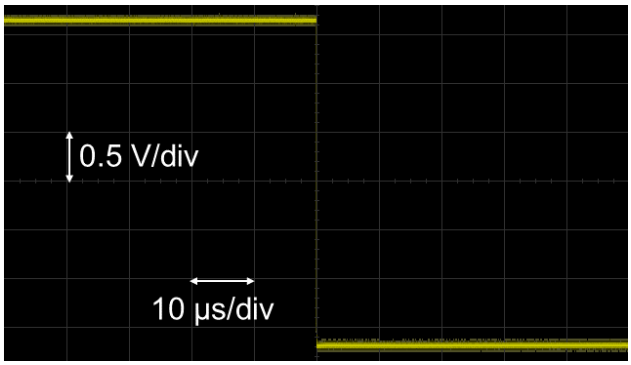

図 7　HTTP GET Flood 攻撃下の波形の軌跡 (mbed LPC1768)

3.3.2　mbed LPC1768 について

実験結果を図 5-7 に示す．Arduino Uno と同様の実験

を行ったが，SYN Flood 攻撃と HTTP GET Flood 攻撃双方において出力される信号にほとんど影響は見られなかった．この主な原因としては，mbed LPC1768 内部で PWM の生成を行うコントローラでの処理が他のモジュールと独立しているため，メインプロセッサとなる Cortex-M3 や通信を行っている Ethernet モジュールに負荷を与えても直接影響を及ぼさなかった可能性が考えられる．通常状態においても波形にほとんど変動していない要因も PWM 生成部が独立しているため，他の処理の影響を受けにくいためだと推測される．また，ハードウェアとソフトウェア処理の実装の違いによって影響の違いが出たことも考えられるが，具体的に処理に差が出た個所を確認するためには検証実験が必要だと考えらえれる．

4. 考察

4.1 ArduinoUNO に関して

Arduino に対しては限定的ではあるものの，出力信号に攻撃によるものと考えられる影響が確認された．制御システムにおいては，一時的な物理ノイズが発生してもシステム全体に影響が出ないように設計されているものがほとんどであるため，瞬間的に発生する物理的な変動はほとんど問題にならないと考えられる．しかし，ランダムに発生するノイズとの違いとして攻撃下においては非常に高い頻度で信号に誤差が生じることがあげられる．この違いがシステムに与える影響については，実際に制御システム使用されている機器を用いて実験を行う必要がある．

4.2 mbed LPX1768 に関して

mbed LPX1768 については出力信号それ自体には攻撃の影響は確認されなかった．先に述べたように処理が独立されていることが主な要因だと考えられる．つまり，デバイスにきわめて大きな負荷がかかる状態であっても，ハードウェアレベルで深く独立して処理を行うシステムでは，その処理能力に関係なく安定して出力信号を生成することができる可能性がある．情報システムと比較して制御システムにおいてはデバイスが安定して動作を続けることは非常に重要であるため，この構成方法は今後ますます重要になると考えらえる．今後は今回実験したデバイスと同程度の処理能力かつ同一の処理系内で出力信号の生成も行うチップを搭載しているデバイスと比較実験を行いその有用性について確認を進めていく必要がある．

4.3 今後の課題

各攻撃下において各デバイスに対して通信を試みたところ正常な通信が不可能になっていた．これは攻撃により通信帯域が圧迫されていたことやデバイスでの処理が追いついていないことなど原因だと考えられる．このような状況下ではネットワークを介して制御通信を送信しても部分的なパケットロスが発生する恐れある．そのためデバイスが制御信号を受けとることができなくなり制御不能に陥る危険性も考えられる．回避策としては各デバイスが一定期間正常な通信が行えなくなったと判断した場合，自動的にフェールセーフに移行するように設定を行うなどの対処が考えられるが，可動性を優先しなければならない制御システムにおいてはシステムが停止することが許容できない場合も想定されるので，今後の課題とする必要が考えられる．

本実験においてはデバイスから出力される信号の波形にのみ注目した．しかし，重要インフラなどで用いられる制御システムにおいては，システムを構成しているデバイスが制御命令通りに出力信号を生成することに加え，応答のリアルタイム性が重要視される場合も多い．そのためデバイスが処理命令を受けてから信号を生成するまでの遅延も考慮する必要があると考えられる．よって今回行った実験と同じ環境下で，制御情報をネットワークを介してやり取りする場合の伝達にかかる遅延と負荷がかかっている状況下でのプロセッサ内で処理の遅延がどの程度発生するのかについても研究を進める必要があると考えられる．

5. まとめ

本稿では，まず制御システムにおけるセキュリティを考える上での問題点を整理し，その上でこれまで研究が行われていなかった出力信号に注目し，攻撃実験を行った．その結果，ArduinoUNO に対しては限定的ではあるが攻撃の影響が観測された．しかし，本研究では実際の制御システムで用いられている装置を対象にしていないので，今後はその影響が深刻な問題となりうるのかについては議論が必要である．また，攻撃の影響が観測されなかった mbed LPX1768 についてはその原因についての考察と，ハードウェアレベルでの処理機能の分離が信号の安定化に寄与する可能性について考察を行った．また今回の実験では出力信号の波形にのみ注目したが，今後は攻撃がデバイスの処理時間にどの程度影響を及ぼすかについて実験を行い，評価する必要がある．

参考文献

[1] UK Government Office for Science: The Internet of Things: making the most of the Second Digital Revolution(2014).

[2] Communication Promoters Group of the Industry-Science Research Alliance, National Academy of Science and Engineering: Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group(2013).

[3] 経済産業省：平成 28 年度経済産業政策の重点 (2015).

[4] 経済産業省：日独 IoT/インダストリー 4.0 協力に係る共同声明への署名を行いました (2016)，入手先 ⟨http://www.meti.go.jp/press/2016/04/20160428011/20160428011.pdf⟩(accessed 2016-8-3)

[5] ICS-CERT: Alert(IR-ALERT-H-16-056-01)Cyber-

Attack Against Ukrainian Critical Infrastracture(2016). 入手先 ⟨https://ics-cert.us-cert.gov/alerts/ IR-ALERT-H-16-056-01⟩(accessed 2016-8-3)

[6] Knownsec Security Team: Maliciaous Code Analysis on Ukraine's Power Grid Incident V4(2016).

[7] IPA：重要インフラの制御システムと IT サービス接続に関する調査,(2009).

[8] Alvaro A Cárdenas, Saurabh Amin, Shankar Sastry : Research challenges for the security of control systems, in HOTSEC' 08:Proceedings of the 3rd conference on Hot topics in security. Berkeley, CA, USA: USENIX Association, pp. 1-6(2008).

[9] 大和田徹, 伯田恵輔, 森田伸儀, 内山宏樹, 萱嶋信：制御・車載システムにおけるセキュリティ機能要件に関する考察, 2015 年暗号と情報セキュリティシンポジウム（SCIS2015）予稿集, 3C3-1(2015).

[10] 田村研輔, 松浦幹太：制御システムにおけるライブフォレンジックの適用可能性に関する実験的評価, 2015 年暗号と情報セキュリティシンポジウム（SCIS2015）予稿集,3C3-5(2015).

[11] Barbosa. Rafeal Ramos Regis, Sadre. Ramin, Pras. Aiko: Flow whitelisting in SCADA networks, *International journal of critical infrastructure protection*, 6(3-4), pp.150-158(2013).

[12] Nickey Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, Ingrid Verbauwhede: Chaskey:An Efficient MAC Algorithm for 32-bit Microcontrollers, *Selected Areas in Cryptography*, SAC 2014, Lecture Notes in Computer Science, vol. 8781. pp. 306-323(2014)

[13] 赤津観：モータ技術のすべてがわかる本, ナツメ社 (2012).