IoTにおける多様なデバイスに適用可能な軽量暗号

岡村 利彦

要 旨

実世界のデータを活用するIoTシステムでは、デバイスからのデータ収集もサイバー攻撃の対象となり、暗号化による対策が重要になります。軽量暗号は、非力なデバイスへの暗号適用の拡大を目指して、小さなフットプリントや計算量を実現する暗号方式であり、国際標準化やガイドライン作成も進んでいます。秘匿と改ざん検出を併せて行う認証暗号は、特に注目され、技術コンペティションCAESARが開催されています。NECは、優れた実装性を持つ軽量ブロック暗号TWINEと認証暗号OTRを開発しており、OTRはCAESARの２次選考を通過しました。

KeyWords　セキュリティ／暗号／認証／軽量暗号／認証暗号

1. はじめに

IoT化によって、さまざまなデバイスがネットワークにつながることで新たな価値が創出される一方で、監視カメラの不正操作や自動車へのハッキングが報告されるなど、IoTのセキュリティ脅威は現実のものになっています。情報処理推進機構（IPA）による「情報セキュリティ10大脅威2017（組織）」でも「IoT機器の脆弱性の顕在化」が８位にランクされました。

暗号化は有効な対策となりますが、IoTにおいては、これまで暗号化を考慮してこなかったセンサーデバイスなど、さまざまな制約のある環境で暗号化を適用することが求められます。軽量暗号は、この課題に応えるべく研究開発されてきた技術です。本稿においては、第２章でIoTのセキュリティ脅威と暗号化による対策、第３章で軽量暗号の要件、技術と動向を説明し、第４章でNECのブロック暗号TWINEと認証暗号OTRを紹介します。

2. IoTのセキュリティ脅威と暗号化による対策

IoTシステムにおいては、デバイスによる実世界からのデータ収集までがサイバー攻撃の対象となることが、セキュリティに関して従来のITシステムと大きく異なる点です。例えば、プラントのIoT化では、生産設備に配置された大量のセンサーからデータを収集、分析してリアルタイムで自律的に制御を行うことで、生産性や保守性を飛躍的に高めることを狙います。このとき、センサーデータの改ざんも誤った分析結果を導き、その結果に基づいて、不正な制御が発生すると大きな被害を引き起こす可能性があります。また、計測データや制御コマンドは、生産や管理にかかわるノウハウとなる企業秘密であり、その漏えいを防ぐことは競争力の点からも重要になります。現在は問題ないとしても、将来的な脅威を想定することも必要になります。

センサーデバイスにおける暗号化は、秘匿と認証（改ざん検出）のデータ保護機能を実現することで、これらの脅威に対しての有効な対策になります（**図1**）。軽量暗号は、

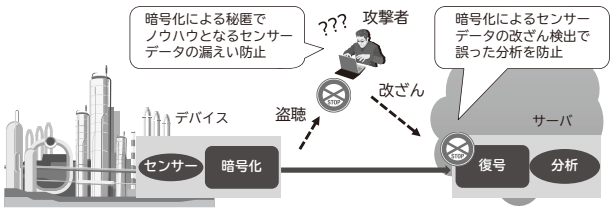


図1　データ収集における攻撃への暗号化による対策

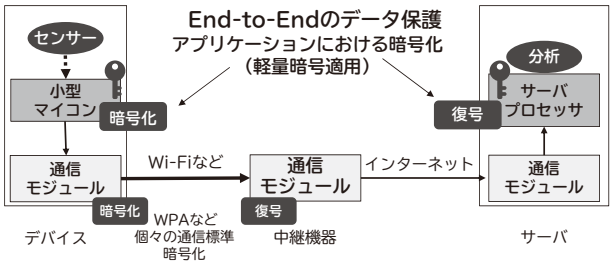


図２　軽量暗号の適用例

リソースの限られたデバイスでも安全な暗号の適用を可能にすることを目指します。

携帯回線など通信標準の暗号化が存在する場合もありますが、このような場合にも、デバイスからサーバまでのend-to-endのデータ保護や通信方式に依存しない安全性を保証するためには、アプリケーションレイヤでの暗号化が有効となります（**図2**）。アプリケーションを処理するプロセッサにおいて、未使用のリソースで暗号化を行う必要があり、できるだけ軽量であることが望まれます。

3. 軽量暗号技術

3.1 軽量暗号の要件

軽量暗号の実装性に関する要件として、次の項目が挙げられます。

・サイズ（回路規模、ROM/RAMサイズ）
・消費電力
・エネルギー消費量（消費電力量）
・処理速度（スループット、遅延）

デバイスへの実装可能性は、第一にサイズで決まります。消費電力はRFIDや環境発電デバイスにおいて、エネルギー消費量はバッテリ駆動のデバイスにおいて、特に重要な項目となります。カメラや振動センサーなどデータの伝送量の多いデバイスでは、高スループットが必要となり、車載システムなどリアルタイム制御処理では、低遅延が重要になります。

消費電力は、ハードウェアの回路規模もしくは使用するプロセッサに大きく依存するため、消費電力に関してもサイズが暗号方式の軽量性の目安となります。エネルギー消費量は、実行時間から処理速度に依存し、処理速度を決める計算量が軽量性の指標となります。スループットに関しては、並列処理への対応にも大きく依存します。

安全性に関して、暗号はシステム全体の安全性の起点となる技術であり、軽量暗号も、現代暗号として十分な安全性を持つと評価された方式を用いる必要があります。実装性を優先して、ブロック長や秘密鍵長を標準暗号よりも小さく設定する場合でも（例えばブロック長64ビット、秘密鍵長80ビット）、その設定で達成可能な安全性を満たすことを評価された方式を、正しく適用することが必要になります。

3.2 共通鍵暗号と公開鍵暗号

暗号は、大きく共通鍵暗号と公開鍵暗号に分けられます。共通鍵暗号は、暗号化と復号で同一の秘密鍵を用いる方式であり、処理は比較的軽く、データそのものの暗号化や改ざん検出に利用されます。一方、公開鍵暗号は、暗号化で利用する公開鍵と復号で利用する秘密鍵が異なり、公開鍵から秘密鍵を推定することが困難という、非対称性を持っています。公開鍵暗号の計算量は、典型的には共通鍵暗号の1,000倍以上と重いですが、非対称性を利用して共通鍵暗号で利用する秘密鍵の共有やデジタル署名に用いられます。

プラントや車載制御システムなど、通信相手がある程度決まっているシステムでは、デバイス間で共有する秘密鍵をあらかじめ埋め込むことも可能であり、このとき共通鍵暗号のみを用いて安全かつ効率の良いデータ保護を実現できます。一方、車車間通信などで動的かつ不特定の相手と暗号化通信を行うためには、公開鍵暗号の利用が有効となります。

本稿では、以下、リソース制約が強いデバイスに対しても、広く適用が可能な共通鍵暗号を主に取り上げます。共通鍵暗号は、ブロック暗号やストリーム暗号などコアとなる関数（暗号プリミティブ）とこれを利用してパケットに対して秘匿や改ざん検出の機能を実現する方式（暗号利用モード）からなります。**図3**に改ざん検出の暗号利用モー

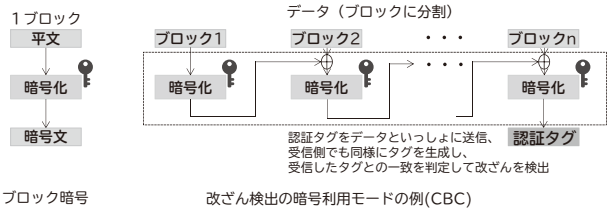


図３　ブロック暗号利用モードの例

ド（メッセージ認証と呼ばれる）の例を、示します。軽量化では、暗号プリミティブだけではなく、暗号利用モードの効率化も必要になります。

3.3 軽量暗号の動向

軽量暗号は、欧州の暗号プロジェクト通じて2004年頃から研究が始まり、M2M/IoTの流れのなかで活発化してきました。国際標準化もISO/IEC JTC 1/SC 27において、ISO/IEC 29192 “Lightweight Cryptography” が定められています。暗号技術の指針を示す米国標準技術研究所（National Institute of Standards and Technology：NIST） も、2013年にLightweight Cryptography Projectを開始し、2017年に軽量暗号の公募をアナウンスしています。

PRESENTは2007年に発表された、軽量暗号の先駆となるブロック暗号であり、ISO/IEC 29192にも登録されています。PRESENTは、標準暗号AESでは不可能なRFIDタグに実装可能なレベルの回路規模を実現しました。米国国家安全保障局（National Security Agency：NSA）は、マイコン実装で非常に小さなROMサイズで実装可能な軽量ブロック暗号SIMON/SPECKを発表し（2013年）、国際標準化を目指して、ISO/IEC29192への追加を提案しています。

秘匿と改ざん検出を合わせて安全かつ効率よく行う暗号利用モードは、「認証暗号」と呼ばれます。IoTにおける改ざん検出の重要性から、今後、暗号化といえば認証暗号化となると予想されます。同一のブロック暗号であっても、認証暗号としての実現方法によって、効率や安全性は大きく変わります。NIST推奨の認証暗号とてAES-CCM/GCMが存在しますが、認証暗号の重要性と研究の進展から、更に軽量で安全な次世代の認証暗号が望まれています。このような状況で、NISTの支援を受けて、研究者コミュニティによる国際的な認証暗号コンペティション CAESAR（Competition for Authenticated Encryption: Security, Applicability, and Robustness）が2014年に始まり、60件の提案がありました。2017年末に、アルゴリズムの特性や目的に応じた次世代方式を選出するために、毎年候補の絞り込みが行われています。

日本国内においては、電子政府推奨暗号の策定や暗号技術の動向を監視するCRYPTREC（Cryptography Research and Evaluation Committees）の軽量暗号WGが、2013年から活動しています。代表的な軽量暗号の実装性の評価と、安全性の調査及び軽量暗号の有効なユースケースの検討などを、進めています。

4. NECの軽量暗号

4.1 ブロック暗号TWINE

NECの軽量ブロック暗号TWINE[1)]は、小規模回路実装を実現しながら、従来の軽量暗号PRESENTで課題のソフトウェア実装性を解決することを目指して設計されました。ブロック長は64ビット、秘密鍵長は80，128ビットの2種類で、PRESENTと同一の設定です。

TWINEは、前述のCYRPTREC軽量暗号WGの評価対象暗号に選ばれており、ハードウェアとソフトウェアともにトップクラスの性能を示しています。以下、軽量暗号WGの評価結果[2)]を元に、TWINEの実装性を紹介します。

ブロック暗号は、実装性を考慮してラウンド関数と呼ばれる同一処理を繰り返すアルゴリズムで構成されます。ハードウェア実装でAES 1ラウンドの回路規模15Kgateに対して、TWINE 1ラウンドの回路規模は、その1/7の2Kgate程度です（PRESENTと同程度）。同一スループットの比較では、TWINEの回路規模は、AESの1/2以下になります。高速通信対応では、暗号化処理も並列化で回路規模が大きくなりますが、TWINEの小規模回路実装性は、このようなケースでも効果を発揮します。

一方、ソフトウェア実装性に関しては、AESが優れており、マイコン（ルネサスRL78）実装に関してROM が1Kバイト以上の場合は、TWINEなど軽量暗号より高速です。しかし、ROMサイズが512バイトの場合には、AESは実装不可能となるのに対して、TWINEは実装可能となります。PRESENTとの比較では、TWINEは2.5倍の処理速度を達成しています。

安全性に関しても、TWINEは、AESと同等の評価で問題がないことを確認しています。2012年の発表以来、解析を試みた論文が発表されてきていますが、安全性評価に影響を与えるものは出ていません。

4.2 認証暗号OTR

一般に、暗号による改ざん検出の計算量は、暗号化（秘匿）と同等であり、NIST推奨の認証暗号AES-CCM/

GCMも計算量は、暗号化の2倍となります。認証暗号の計算量は、暗号化のみの計算量以上であるため、暗号化のみと同等の計算量が認証暗号の理論的限界となります。

この理論的限界を満たす認証暗号として、OCBが存在しますが、復号処理において、OCBは、ブロック暗号の復号関数を必要とします。一方、AES-CCMが復号処理もブロック暗号の暗号化関数で構成しているように、構成要素が少ないほど、サイズを小さくすることが可能になります。NECが開発したOTR[3]は、計算量の理論的限界をブロック暗号の暗号化関数のみで実現する、世界初の認証暗号です。OTRは、前述の認証暗号コンペティションCAESARに提案されており、1次選考（2015年）の30件に続いて、2次選考（2016年）の15件にも選出されました。

図4に、OTRのアルゴリズムを示します。OTRの改ざん検出処理（認証タグ生成）は、データのブロック単位のチェックサムの暗号化であり、データ長によらず1ブロックの暗号化で実現できます。暗号化は、2Rフェイステルと呼ばれる構造を用いており、復号も暗号化と同じように、ブロック暗号の暗号化関数を用いて実現できます。

OTRの安全性は、ブロック暗号の安全性に基づいて理論的に証明されています。また、OTRは、任意のブロック暗号と組み合わせることが可能です。AESとの組み合わせでは、AESのこれまでの豊富な実装資産を活用することができ、CAESARにも“AES-OTR”を提案しています。一方、TWINEとの組み合わせ“TWINE-OTR”は、AES-OTRと比べてサイズの一層の削減が可能になります。

NECは、名古屋大学ほかと共同で認証暗号CLOC/SILCも開発しており、CLOC/SILCは、小さなデータサイズに対して計算量のオーバーヘッドが小さいという特長があります。CLOC/SILCもCAESARに提案され、2次選考を通過しています。

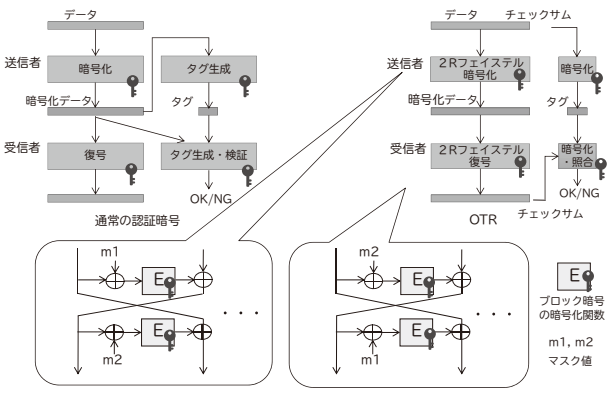


図4　OTRアルゴリズム

5. おわりに

本稿では、IoTの省リソース環境でも適用可能な軽量暗号について、NECの軽量暗号を中心に紹介しました。軽量暗号も実際に適用する際には、鍵管理の機能や運用を考慮する必要があり、NECでは、鍵更新や鍵交換を含めた軽量な暗号ライブラリの開発から実用化の促進を図っています。また、公開鍵暗号による鍵交換の軽量化を目指した研究も進めています。今後も、このような暗号技術の研究を通じて、セキュアのIoTシステムの実現に貢献していきます。

参考文献

1) T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi：TWINE：A lightweight block cipher for multiple platforms, SAC 2012.
2) CRYPTREC：暗号技術調査WG（軽量暗号）報告書, 2015.3 https://www.cryptrec.go.jp/estimation/techrep_id2406.pdf
3) K. Minematsu：Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions, EUROCRYPT 2014

執筆者プロフィール

岡村 利彦
セキュリティ研究所
主任研究員

関連URL

NEC、IoTでつながる多様なセンサや機器で利用可能な認証暗号技術を開発，2015.7
～　データ処理量を従来比　約1/2に低減　～
http://jpn.nec.com/press/201507/20150721_04.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.70 No.1　デジタルビジネスを支えるIoT特集

デジタルビジネスを支えるIoT 特集によせて
デジタルビジネスを支えるNECのIoT 事業

◇ 特集論文

IoTを支えるプラットフォーム

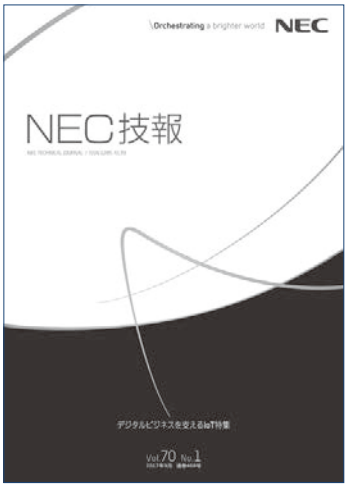
ビジネス変革を支えるIoTプラットフォーム「NEC the WISE IoT Platform」
IoTの顧客価値を支えるエッジコンピューティング
IoTのミッシングリンクをつなぐエッジコンピューティング技術
エッジコンピューティングのソリューション事例

お客様に価値を提供するIoTソリューション

IoT時代のものづくり「NEC Industrial IoT」
作業効率化と品質向上を同時に実現する画像・重量検品ソリューション
AI技術「自律適応制御」を用いた倉庫人員最適配置ソリューション
ヒアラブル技術によるヒューマン系IoTソリューションの取り組みと展望
パブリックセーフティを支える映像配信技術
IoT・AIによる小売業の革新
工場機器をリアルタイムに遠隔制御する無線ネットワーク技術：無線ExpEther
IoTにおける多様なデバイスに適用可能な軽量暗号
NECの生産拠点における需要予測の取り組み　～AI×エスノグラフィによる現場定着～

◇ 普通論文

画像認識技術を活用したマイナンバー収集サービス



Vol.70 No.1
（2017年9月）

特集TOP