2F-02

IoT機器向けセキュリティ技術

小林 正明† 北沢 淳郎† 田中 恵梨香† 安達 駿† 武藤 浩二†
パナソニック株式会社†

１．はじめに

IoT 機器の活用により生産性や利便性の向上が期待され，IoT 機器の普及が急速に進んでいる．一方で，セキュリティが脆弱な IoT 機器がインターネットにつながることで，IoT 機器を標的としたサイバー攻撃も急増している[1]．IoT 機器に対するサイバー攻撃は，人命，財産に直結する場合も多いため，大きな被害が発生する可能性がある．従って，サイバー攻撃を防ぐために，IoT 機器にも強固な暗号・認証機能を実装するとともに，暗号・認証機能で防ぎ切れないサイバー攻撃を検知し，早期に対策することが重要である．

本稿では，IoT 機器における暗号・認証機能，及びサイバー攻撃検知機能の実現方法について検討したので，その結果を報告する．

２．IoT 機器向けセキュリティの課題

サイバー攻撃とは，不正アクセスにより IoT 機器に侵入し，データの不正取得，改ざん，機能妨害をする行為である．不正アクセスの手口には，(a) IoT 機器の認証機能を突破する方法と，(b) IoT 機器に実装されたアプリケーションの欠陥（セキュリティホール）を利用する方法がある．(a) を防ぐためには公開鍵暗号方式を用いた PKI（Public Key Infrastructure）による暗号・認証が有効である．また，(b) を防ぐためには，サイバー攻撃を早期に検知して，アプリケーションの更新などの対策をとる必要がある．

２．１　シード生成機能の課題

PKI による暗号・認証を実現するために，IoT 機器は図１に示すように，安全な通信を行う暗号・認証機能，暗号・認証鍵を生成する鍵生成機能，鍵生成に必要な擬似乱数生成機能，擬似乱数の種（初期値）を与えるシード生成機能から構成されている．攻撃者はセキュリティ的に弱い部分から侵入を試みるため，暗号・認証機能が強固であっても，例えば暗号・認証に利用

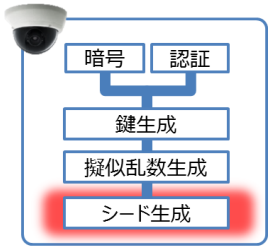

図１．IoT 機器のセキュリティ機能の構成

する鍵やシードが漏えいすると，サイバー攻撃は可能となる．

ここで，暗号・認証機能，鍵生成機能，擬似乱数生成機能には，政府推奨暗号等の安全性が確認された方法が公開されているが，シード生成機能について具体的な実装方法は規格化されていない．また，暗号・認証に用いる鍵を IoT 機器の外部で生成すると，鍵の漏えいリスクが高まる．そのため，鍵生成に必要な推測不能なシードを IoT 機器の内部でどのように生成するかが課題となっている．

２．２　サイバー攻撃検知機能の課題

アプリケーションは利便性向上のための改善を続けるため，新たなセキュリティホールを完全になくすことは難しい．また，サイバー攻撃も日々進化を続けているため，図２に示すような仕組みを用いてサイバー攻撃を早期に検知することが重要となる．

IT セキュリティでは，PC とネットワーク機器から収集したログを一元管理，分析する SIEM（Security Information and Event Management）でサイバー攻撃を検知する．しかし，誤検知や判断の難しい攻撃もあるため，最終的にはサイバー攻撃の検出や分析を行う専門組織である SOC（Security Operation Center）で，高度なスキルを保有する人材が判断する．

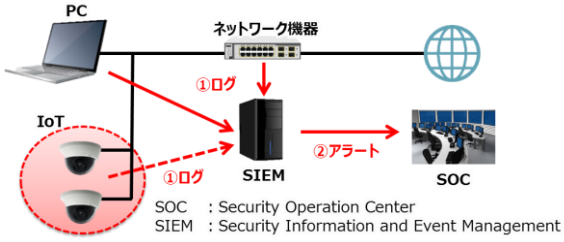

図２．攻撃検知の仕組み

Security Technology of IoT Devices
† Masaaki Kobayashi, Atsurou Kitazawa, Erika Tanaka, Shun Adachi, Kouji Mutou
† Panasonic Corporation

このような攻撃検知の仕組みの中で，ネットワーク機器は事前登録されたシグネチャとパケットのマッチングなどで攻撃を検知しているが，攻撃手法が進化すると，対応は難しいものとなる．また， PC とネットワーク機器のログだけでは，ネットワーク機器を経由しない IoT 機器間の通信による横感染を防ぐことは難しい．IoT 機器からログを収集し，エンドポイントの状況を把握できれば，これらの問題は解決しやすくなるが，IoT 機器の通常動作や通信に影響を与えずにログ収集するのは容易ではない．

３．シード生成機能

IoT 機器の内部で生成されたシードが推測不能であるか，図３に示すようにデジタルノイズ源の出力をエントロピー評価して判断するように定められている[2]．また，シード生成に利用できるアナログノイズ源としては，実行パイプライン，CPU とメモリバスのクロックスピードの違い，分岐予測ユニットなど，いくつかのジッターが PC で検討されている[3]．しかし，IoT 機器においてこれらのジッターが推測されない十分なエントロピーを持っているか，検討はされていない．

そこで，デジタルノイズ源からジッターを効率よく抽出する方法を検討し，IoT 機器で広く使われるいくつかの評価環境（CPU：ARM9，ARM Cortex-A8，OS：Linux）でエントロピー評価を実施した．評価の結果，IoT 機器でも推測不能なエントロピーが取得できることを確認した．

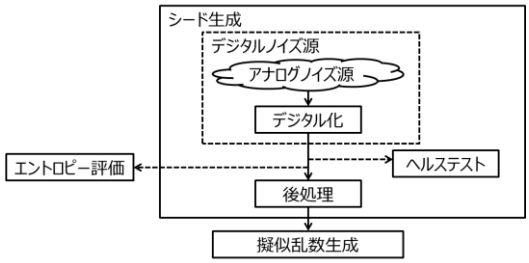

図３．シード生成機能の構成と評価モデル

４．サイバー攻撃検知機能

IoT 機器に暗号・認証機能を実装し，PC と同じように PKI による暗号・認証ができれば， 残る IoT 機器へのサイバー攻撃手法は PC と同様にセキュリティホールへの攻撃となる．ここで，サイバー攻撃を SIEM で検知するために， PC と同等のログを IoT 機器から出力しようとすると，ログ量が多く，IoT 機器の通常動作や通信に影響を与える可能性がある．

そこで，攻撃検知に用いるログ量を２つのアプローチで絞り込む検討を行った．１つは少ないログで効率よく攻撃を検知できる検知アルゴリズムを実現すること，もう１つは攻撃検知アルゴリズムに必要不可欠なログのみを収集できるように，IoT 機器側から出力するログの種別やタイミングを絞り込むことである．

攻撃者の視点でサイバー攻撃のシナリオを分析することで，攻撃者が必ず実施する主要な不審手順を洗い出し，これらの不審手順を検知することで，進化する攻撃も含めて，少ないログで効率良く攻撃を検知するアルゴリズムが実現できる．

また，検知アルゴリズムに必要なログのみを出力できるように，IoT 機器側から出力するログを削減することで，IoT 機器の通常動作や通信に影響を与えずにログ収集ができるようになる．評価の結果，IoT 機器で広く使われるいくつかの評価環境（CPU：ARM Cortex-A8，ARM Cortex-A9，OS：Linux）で通常動作や通信に影響を与えずに，ログ収集，攻撃検知ができることを確認した．

５．まとめ

IoT セキュリティの課題となっているシード生成機能と，サイバー攻撃検知機能が IoT 機器に実装できることを確認した．今回は OS として Linux が動作する CPU での評価を実施したが，今後は RTOS が動作する CPU も評価を行う予定である。また，アナログノイズ源として利用される各種ジッターから，エントロピーが取得できる条件についても詳細な調査を行う予定である．

なお，本研究の一部は，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：国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO））によって実施されている．

参考文献

[1] 後藤篤志, “「IoT セキュリティ総合対策」について,” https://igcj.jp/meetings/2017/1130/igcj22-1-4-goto.pdf, 参照 Jan. 7, 2019.

[2] NIST Special Publication 800-90B, “Recommendation for the Entropy Sources Used for Random Bit Generation,” Jan 2018.

[3] S.Muller, “CPU Time Jitter Based Non-Physical True Random Number Generator,” http://www.chronox.de/jent/doc/CPU-Jitter-NPTRNG.pdf, 参照 Jan. 7, 2019.