IoT機器のための暗号・認証技術，およびサイバー攻撃検知，対策技術

Technology for Encryption, Authentication, Cyber-Attack Detection, and Cyber-Attack Prevention Measures for IoT Devices

松　尾　正　克　Masakatsu Matsuo
古賀田勝則　Katsunori Kogata
田　中　裕　之　Hiroyuki Tanaka
武　藤　浩　二　Kouji Mutou
小　林　正　明　Masaaki Kobayashi

要　旨

IoTの活用により生産性や利便性の向上が期待されるが，多種多様な機器がインターネットに繋（つな）がることにより，サイバー攻撃の被害増大が懸念されている．サイバー攻撃を防ぐためには，ITだけでなく組み込み機器にも暗号・認証機能を実装し，加えて，進化する攻撃を検知して対策することが重要である．当社は，長年にわたり組み込み機器のセキュリティ技術でさまざまな研究を行い，ITと比べリソースの少ない組み込み機器で暗号・認証機能を実装する方法，およびそれをベースにサイバー攻撃を検知，対策する基盤を実現した．

Abstract

While it is possible to improve productivity and convenience by using the IoT, there is a concern that damage caused by cyber-attacks will increase among the various devices connected to the Internet. To prevent cyber-attacks, it is important to implement encryption and authentication functions not only in IT infrastructure but also in embedded devices. In addition, it is important to detect evolving attacks and to adopt countermeasures. For many years, we have conducted various kinds of research in embedded security technology, and have realized a method for implementing encryption and authentication functions using fewer resources than would be required by an IT infrastructure for built-in equipmentand platform for cyber-attack detection and countermeasures based on such technology.

1. はじめに

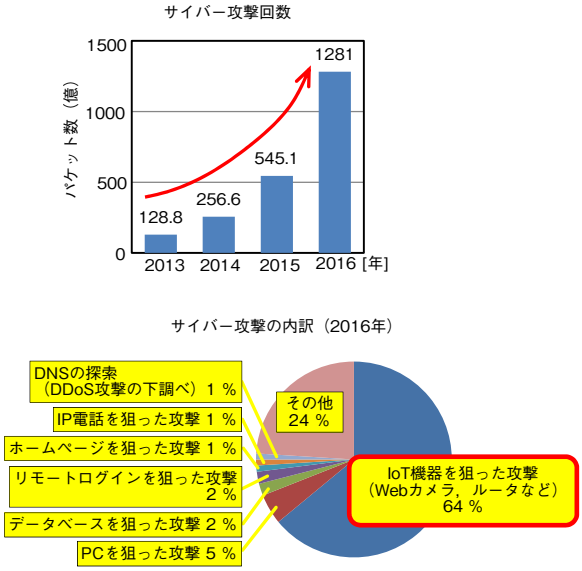
あらゆる物（端末）がインターネットに繋がるIoT（Internet of Things）は，生産性やサービスの利便性を飛躍的に向上させる第四次産業革命の起爆剤として大きな期待を集めている．一方，PC（Personal Computer）機器を中心に構成されるITとは異なり，組み込み機器（以下，IoT機器と呼称）がインターネットに繋がるIoTは，セキュリティ的に脆弱（ぜいじゃく）で，ハッキングによる被害増大が懸念されている．

当社は，10年以上にわたり，IP（Internet Protocol）電話，IP-PBX（Internet Protocol - Private Branch eXchanger），ネットワークカメラ，決済端末など多数のIoT機器を開発するなかで，いち早くこのIoTセキュリティの課題に直面し，これを克服してきた経験を有する．

本稿では，IoT機器のサイバーセキュリティの現状と本質的な課題を解説し，IoT機器に求められる暗号・認証機能の実装方法，およびサイバー攻撃検知，対策機能の実現方法について，当社の取り組み内容を紹介する．

2. IoTセキュリティの現状

第1図に示すように，IoTの普及とともにハッキング件数も急増し，攻撃の2/3はIoT機器を標的としている[1]．ハッキング手法も高度化し，これまで安全と見られていた産業機器でも被害が発生しており，どのようなIoT機器ももはや安全とは言えない状況である．人命や財産に直結する車や家電もインターネットへの接続が進んでおり，IoT機器の脆弱性は深刻な社会的問題になりつつある．



第1図　サイバー攻撃の回数と内訳

Fig. 1　Number and breakdown of cyber-attacks

3. IoTセキュリティ特有の課題

サイバー攻撃とは，インターネットに接続された機器に対して，なりすましなどの不正アクセスにより侵入し，データの不正取得，改ざんする行為や，システムの機能を妨害する行為である．不正アクセスの手口には，(a) パスワードなどの認証機能を突破する方法，(b) アプリケーションの欠陥（セキュリティホール）を利用して侵入する方法がある．(a) を防御するためには，公開鍵暗号方式を用いたPKI（Public Key Infrastructure）により通信相手を認証することが有効である．また，(b) を防ぐためには，攻撃を早期に検知し，アプリケーションを更新するなどの対策をとる必要がある．

このような現状に対して，さまざまなIoTセキュリティ技術が登場している．このなかには，ITセキュリティ技術を単純に活用したものも散見される．しかし，IoTセキュリティには，防御・検知・対策の観点で以下に示す課題があり，単純な活用は適切とは言えない．

① 防御（暗号・認証）における課題

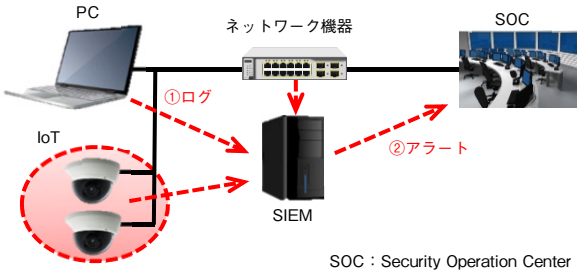
暗号・認証は，攻撃者に莫大（ばくだい）な解読コストや解読時間を強いることで安全性を確保している．したがって，暗号・認証の安全性はその計算処理量で決まる．攻撃者は多数のPC機器を用いて解読を試みるので，安全を確保するには，政府推奨暗号のような膨大な計算処理を施す暗号・認証方式が必要となる．

一方で，このような暗号・認証方式は高速処理が求められるが，ハードウェアで実装するとコストアップになり，脆弱性が発見されたときの入れ換えも困難である．そのため，ソフトウェアによる実装が望まれるが，IoT機器は，CPU（Central Processing Unit）性能やメモリーサイズを抑えたものが多く，その実装は容易ではない．

② 攻撃検知における課題

アプリケーションは利便性を向上するために高度化，複雑化を続けるため，新たなセキュリティホールが完全になくなることはない．しかも，サイバー攻撃は日々進化するため，暗号・認証機能だけでハッキングを完全に封じ込めるのは困難である．したがって，被害拡大を防ぐためには，**第2図**に示すような仕組みを用いてサイバー攻撃の早期検知が重要となる．

ITセキュリティでは，PC機器におけるウィルス検知や，ネットワーク機器からのログをSIEM（Security Information and Event Management）で分析することによりサイバー攻撃の検知を行う．SIEMでは，ファイアウォールなどのネットワーク機器が出力する多様で膨大なログを一元管理し，分析することで，リアルタイムに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，最終的にはネットワークやデバイスを監視し，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）において，高度なITセキュアスキルを保有する人材が判断を行う．



第2図　攻撃検知の仕組み
Fig. 2　Attack detection structure

多岐にわたる知識・経験を要するこのような人材は育成が難しく，常に不足気味である．ここにIoT機器が検知対象として加わると，ITセキュアスキルに加え，IoT機器の知識も必要となるため，人材育成はさらに困難なものになる．また，IoT機器は台数も膨大でログ量も急増するため，現有の人材でSOCを運用するのは容易ではない．

③ 攻撃対策における課題

PC機器と異なり，IoT機器は10年以上使用されるものが多い．長期になれば，暗号・認証の危殆（きたい）化やハッキング手法の高度化で，バージョンアップ機能が必須となる．IoT機器でもPC機器のように，リモートメンテナンスやソフトウェアの自動アップデートを実施することが望ましいが，①に記述したように，一般のIoT機器は暗号・認証機能が弱いため，このような仕組みを実装すると，逆に攻撃者にマルウェアを送り込まれるなど悪用される危険性が伴う．

④ 求められる『説明責任』

従来，IoT機器の製造者やユーザーは，ハッキングでは被害者になるケースが大半であったが，Mirai[2]のように，脆弱なIoT機器をハッキングし，これを踏み台に，他のシステムを攻撃するケースでは，このようなIoT機器を放置した加害者という立場であり，訴訟リスクがある．

また，IoT機器では，PC機器と異なりユーザーの秘情報である暗号鍵や認証鍵をメーカーが設定するケースが多く，責任分解点（責任範囲を切り分ける境界）があいまいで，被害発生時に係争になるおそれが強い．

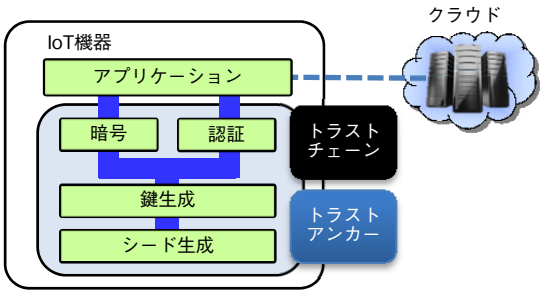
したがって，IoTセキュリティでは，①～③の対策を含め，各セキュリティ対策において，常に安全性の根拠，すなわちより所を示すことが求められる．

4. 防御（暗号・認証）に対する当社の取り組み

この章では，防御（暗号・認証）に対する「説明責任」の考え方を示し，次に，当社の取り組み内容を紹介する．

4.1 『説明責任』を果たすサイバー防御対策

IoT機器は**第3図**に示すように，機器固有の機能を実現するアプリケーションソフトウェア，その安全な通信を保障する暗号・認証機能，それに利用される暗号・認証鍵を生成する鍵生成機能，その鍵の種（初期値）を提供するシード生成機能など，複数のコンポーネントで構成されている．そして，セキュリティ的にはアプリケーションソフトウェアは暗号・認証機能に守られ，その暗号・認証機能は鍵生成機能に守られ，その鍵生成機能はシード生成機能に守られる仕組みになっている．



第3図　IoT機器のセキュリティコンポーネント
Fig. 3　Security components of an IoT device

ここで，シード生成機能のように，すべてのコンポーネントの安全性の根拠となるコンポーネントをトラストアンカー，そのトラストアンカーに繋がるコンポーネントをトラストチェーンと呼ぶ．攻撃者はセキュリティ的に最も弱い部分から侵入を試みるため，たとえば，攻撃者に暗号・認証鍵やシード値を暴かれると，暗号・認証機能が強固なものであっても，ハッキングは可能となる．言い換えると，政府推奨暗号のような強固な暗号・認証機能を実装したとしても不十分で，説明責任を果たすためには，トラストアンカーからトラストチェーンまですべてのコンポーネントで安全性の根拠を示す必要がある．

SQLインジェクション事件[3]のように，メーカーはセキュリティ対策を実施することを，暗黙的に期待されており，メーカーに善管注意義務（善良な管理者の注意義務）が課せられるなか，このような考え方は，防御（暗号・認証）機能の責任分解点を明確にし，訴訟リスクを低減することができる．また，各コンポーネントの安全性の強弱を「見える化」でき，防御対策の費用対効果の向上も期待できる．

4.2 アプリケーションの攻撃対策

IoT機器は，PC機器と異なり運用に人が介在しない場合が多いので，メールに添付されたマルウェアから感染するようなハッキングは受けにくい．一方，IoT機器は，PC機器と同様にアプリケーションに脆弱性が存在する場合があるので，バッファーオーバーフロー攻撃のようなハッキングを受ける可能性がある．この対策については5章，6章で解説する．

4.3 暗号・認証

当社はCPUパワーの劣るIoT機器でも，PC機器と同等の安全な暗号・認証アルゴリズムを利用するため，長期にわたり，暗号・認証の高速計算処理アルゴリズムの研究に努めてきた．その成果は，当社の取り組み内容[4]として解説したので詳細は割愛するが，当社の暗号・認証ソフトウェアモジュールは省メモリーで高速処理性能に優れるため，多くのIoT機器で政府推奨暗号が実装可能である．政府推奨暗号は，安全性の根拠が明確でハッキング被害や訴訟リスクを低減させる効果が大きい．このモジュールは，第三者認証のFIPS（Federal Information Processing Standardization）140-2，CAVP（Cryptographic Algorithm Validation Program），およびCMVP（Cryptographic Module Validation Program）認証も取得している．

4.4 鍵生成

サーバとIoT機器間の機器認証は，秘匿性や運用性の観点で，PKI（Public Key Infrastructure）など公開鍵認証方式の利用が望ましい．機器認証でいまだに鍵長の短いパスワード認証が多く利用されているが，簡単にハッキングできて非常に危険である．

公開鍵暗号には，RSA暗号，DH暗号，楕円（だえん）曲線暗号など複数の方式が存在するが，歴史的な背景や他の機器・システムとの接続のしやすさから，ビジネスではRSA暗号が利用されるケースが多い．

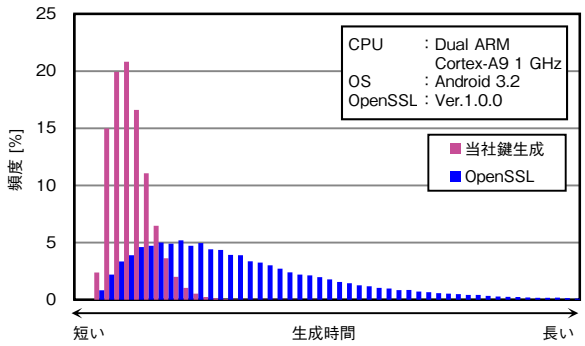
RSA暗号の鍵は巨大な素数から生成される．したがって，RSA暗号の場合，鍵生成とはこの巨大な素数を探索することにほかならない．つまり鍵生成では，あるシード（初期）値，すなわち最初の素数候補が与えられたなら，それが素数か否かを判定し，素数でなければ，次の素数候補を判定するというように，素数を探索し続ける．

素数はすぐに見つかることもあれば，素数砂漠と表現されるように，すぐには発見できないこともあり，素数探索時間は大きくばらつく．CPUパワーの劣るIoT機器では，このばらつきはさらに大きくなる．

IoT機器は，出荷する前に認証鍵を設定する必要があるため，1工程の作業時間が決められた工場では，作業時間

のばらつきが大きいと支障となる．高速なPC機器で鍵を生成しIoT機器にその鍵を書き込めば，作業時間の問題は解決するが責任分解点はあいまいになる．機器の外部で生成した鍵でハッキング被害が発生すれば，メーカーは原因が鍵情報の漏えいでないと証明しなくてはならないが，容易なことではない．また，外部からIoT機器の鍵を書き換えられるこのような仕組みは，攻撃者に悪用される危険がある．

当社は素数判定でも独自の高速計算手法を研究し，**第4図**に示すように，オープンソースに比べ，処理時間のばらつきを1/10程度に抑え,最大生成時間が100秒程度速い，高速鍵生成技術を開発した．鍵生成の時間的ばらつきが少ないので，工場でIoT機器自体が鍵生成を行うことが可能である．また，IoT機器自体が機器の内部で鍵生成を行い，鍵が機器の外部に一切出ないので，鍵生成における責任分解点のあいまいさはない．



第4図　鍵生成の処理速度比較
Fig. 4　Comparison of key generation speed

4.5　シード生成

シード生成は鍵生成機能や乱数生成機能にシード値（種）を提供するトラストアンカーであり，セキュリティ上，非常に重要なコンポーネントである．シード値を入手できれば，暗号・認証鍵は計算で導けるので，政府推奨暗号を利用していてもハッキングは容易である．

したがって，シードを固定値やMAC（Media Access Control）アドレスのような規定値とすると，規定値が暴露された時点で，そのIoT機器を利用したシステムのセキュリティは直ちに崩壊する．それ以上に問題なのは，この規定値を知りうる攻撃者から，密（ひそ）かにハッキングを受けている可能性を否定できないことである．ハッキング被害が発生すれば，メーカーは原因が情報漏えいでないことを証明しなくてはならず，シードが規定値の場合，対処に困ることになる．なお，PC機器では，鍵生成やシード生成はユーザーが実施するので，このような問題は生じにくい．

以上のことから，IoT機器では，誰もが知りえない方法でシード値を生成することが求められる．当社は，IoT機器の内部で，誰も知りえない自然界のゆらぎからシード値を生成する手法の研究，およびガイドライン化の検討を進めている．以下にその一部を紹介する．

＜目標＞

① IoT機器は一般的にセンサなどの特別な測定機器は搭載していないので，ゆらぎは，CPUやメモリーから取得する．

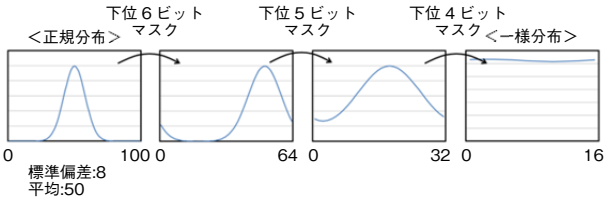
② ゆらぎが不十分であると，複数のIoT機器でシード値が同じになり，その結果，同じ暗号・認証鍵が生成され危険であるため，十分なゆらぎを確保する．

③ 評価に大量のサンプリングデータが必要で[5]，データ取得に時間がかかるため，生成速度を高速にする．

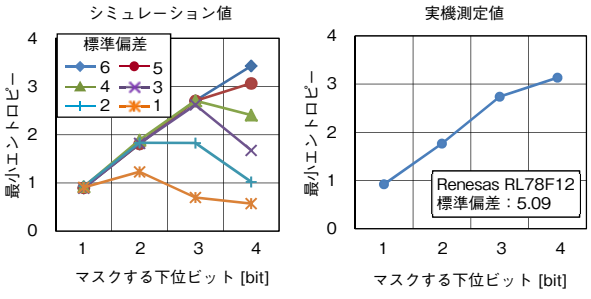
＜研究内容＞

オシレータやメモリーアクセスの時間にはゆらぎがあり，これらのゆらぎから取得したデータの最下位ビットはシード生成に利用できることが知られている[6]．しかし，高速にシードを生成するためには，利用可能なビット（有効ビットと呼ぶ）を効率良く活用する必要がある．

オシレータやメモリーアクセス時間のゆらぎは正規分布で近似できる．ここで，**第5図**に示すように，正規分布の下位ビットを適切にマスクすると正規分布が一様分布に近づく．また，シミュレーションの結果，**第6図**に示すように，正規分布の標準偏差と利用可能なビットには相関があり，標準偏差が大きいほど下位ビットのマスクサイズを大きくしても最小エントロピーは大きくなる．



第5図　有効ビットと分布の関係
Fig. 5　Relation between effective bit and distribution



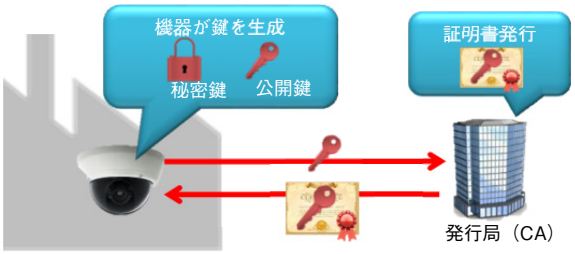
第6図　有効ビットと最小エントロピーの関係
Fig. 6　Relation between effective bit and minimum entropy

そこで，標準偏差から有効ビットを推定し，連結することで効率良くシードを生成する方法を検討した．**第6図**の右図に示すように，幾つかの実機でも検証を行い，シミュレーションと同等の最小エントロピーが得られることを確認した．この結果，有効ビットがNビットのとき，シードの生成もN倍高速になり，十分なエントロピーも確保できることを確認した．

4.6　デバイス証明書発行サービス

当社は，説明責任を果たすために，シード生成，それに続く鍵生成ともに人を介入しない仕組みを実現した．さらにこの利点を活（い）かし，**第7図**に示すように，デバイス証明書（IoT機器のデジタル証明書）でも安全な自動発行サービスを実現し，既に複数の製品で活用している．この仕組みは，秘密鍵をIoT機器の外部に出さずに実現できるので，鍵情報は漏えいしない．

① 工場内で，IoT機器自らがシード値を生成し，そのシード値から認証鍵（公開鍵・秘密鍵）を生成する．
② IoT機器はこの公開鍵を当社のクラウドを経由して，CA（Certification Authority）局に送信する．
③ CA局は，公開鍵をCA局の秘密鍵で署名し，つまりデバイス証明書を作成し，当社クラウドを経由してIoT機器に送信する．



第7図　証明書発行サービス
Fig. 7　Certificate issuance service

5. サイバー攻撃検知に対する当社の取り組み

これまでに説明してきたように，IoT機器には，防御（暗号・認証）機能で，PC機器にないセキュリティ的な課題が存在する．しかし，当社の技術やサービスを適用すると，防御機能に関しては，PC機器とほぼ同等になる．したがって，IoT機器のハッキング手法はPC機器と同様，アプリケーションの脆弱性を攻撃するものになる．そのため，IoT機器がSIEMと連携できれば，PC機器と同様に，SOCから見て現有の人材で扱えるものとなる．

そこで当社では，**第8図**に示すように，IoT機器とSIEMを連携させる攻撃検知モジュールを開発している．IoT

第8図　攻撃検知サービス
Fig. 8　Attack detection service

機器は台数が多いため，PC機器と同じ仕組みでSIEMと連携すると，ログ量やアラート数が急激に増加し，SOCでの対応が困難になる．そこで，少ないログで精度良く攻撃を検知し，攻撃されたIoT機器を特定するために，ログ種別の選定と検知ルールの開発を行っている．また，収集したログに改ざんのおそれがあるとサイバー攻撃検知自体が成り立たなくなるため，先に解説した防御機能をIoT機器に実装したログ収集の仕組みも検討している．

6. サイバー攻撃対策に対する当社の取り組み

IoT機器はメンテナンスが困難な場所に設置されるケースが多い．したがって，サイバー攻撃を受けた際の初動対応や，脆弱性の修正のために，リモートから即時通信を遮断したり，設定変更やバージョンアップができると利便性が高い．

リモートから指示する場合，通信路上に，NAT（Network Address Translation）やFW（Fire Wall）が設置されているケースが多いので，NAT越え（トラバーサル）技術が必要となる．当社は，これをクラウド基盤として整備し，いつでもPC機器など端末機器からリモートでIoT機器に対して，メンテナンスできる仕組みを実現した．

この仕組みのセキュリティ的な問題は，通信を中継するクラウド基盤からの情報漏えいや不正アクセスである．当社のリモートメンテナンスは，先に解説した防御機能をIoT機器に実装することで，端末機器とクラウド間，IoT機器とクラウド基盤間で認証を行うだけでなく，End to End（端末機器とIoT機器）でも暗号・認証を行うことができ，通信路上におけるセキュリティホールからの情報漏えいや不正アクセスを防ぐことができる．

7. トータルサイバーセキュリティの実現

オフィスや工場，医療，学校など多くの組織では，PC機器やIoT機器が混在しており，IoT機器のみを安全にしてもセキュリティ対策は完結しない．また，当社の技術を搭載できない既設のIoT機器の対策も課題である．

当社では，IoT機器に対してソフトウェアで実現可能な防御機能，サイバー攻撃の検知機能，対策機能を実現し

た．そこで，IoT機器のセキュリティ技術に対する当社のアドバンテージを活かし，セキュアコンサル，セキュリティ診断，SOCベンダー，異なるプロトコルのネットワーク間の相互通信を可能とするGW（Gateway）端末メーカー，サイバー攻撃を統合的に検知・排除するUTM（Unified Threat Management）機器などを取り扱うセキュアネットワークアプライアンスメーカーや，保険会社などとアライアンスを組み，IT，IoTのどちらもサポート可能なトータルサイバーセキュリティサービスの実現に努めている．たとえば，攻撃検知では，PC機器，IoT機器の両方の攻撃を検知するサービスを用意した．このサービスは，PC機器とIoT機器の両方で攻撃に対する相関を分析できるので，攻撃の検知率も向上する．

また，当社の技術を搭載できない既設のIoT機器には，当社の防御，検知，対策機能を搭載したGW端末を用意した．既設のIoT機器はこのGW端末を介してネットワーク通信することで，セキュリティを確保できる．

以上の取り組みにより，当社の技術を搭載したIoT機器だけでなく，既設のIoT機器やPC機器が混在するネットワーク環境でも，既知，未知のサイバー攻撃を防ぎ，安全にシステムを運用できるようにした．

8. まとめ

当社は，IoT機器特有のセキュリティ課題について，コンポーネントごとに安全性の根拠を説明できるセキュアモジュールを開発し，PC機器同等レベルの防御機能を実現した．また，防御機能だけでは防ぎきれないアプリケーションの脆弱性を突いた攻撃に対して，攻撃検知機能やリモートメンテナンス機能も開発した．これにより，PC機器やIoT機器が混在する環境でも，サイバー攻撃をトータルに防御・検知・対策できるサービスを整えた．また，ユーザーの使い勝手を向上させるために，いろいろなベンダーとアライアンスを組み，このサービスをトータルサイバーセキュリティとしてパッケージ化した．

今後は， IoT機器へのセキュリティ技術を広く社会普及させ，サイバー攻撃の被害拡大を防ぐために，IoTセキュリティエコシステムを形成するためのガイドラインの策定と，IoT機器がガイドラインどおりに実装されているか評価する方法の研究を進めていく．

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 Apr. 20, 2018.
[2] 小林稔, “Mirai Botnetの検知と対策,” Internet Infrastructure Review, vol.33, pp.18-24, Dec. 2016.
[3] 岡村久道, “この1年のサイバーセキュリティ関連の立法と裁判例, ” 第19回サイバー犯罪に関する白浜シンポジウム, 田辺, May 2015.
[4] 田中裕之 他, “音声・映像機器の暗号技術,” パナソニック技報, vol.59, no.2, pp.109-114, 2013.
[5] NIST Special Publication 800-90B, “Recommendation for the Entropy Sources Used for Random Bit Generation,” Jan. 2018.
[6] 橋本昌宣, “乱数品質を保証したオンチップハードウェア乱数発生器の開発,” ICTイノベーションフォーラム2013, 千葉, Oct. 2013.

執筆者紹介


松尾　正克　Masakatsu Matsuo
コネクティッドソリューションズ社
イノベーションセンター
Innovation Center, Connected Solutions Company


古賀田　勝則　Katsunori Kogata
コネクティッドソリューションズ社
イノベーションセンター
Innovation Center, Connected Solutions Company


田中　裕之　Hiroyuki Tanaka
コネクティッドソリューションズ社
イノベーションセンター
Innovation Center, Connected Solutions Company


武藤　浩二　Kouji Mutou
コネクティッドソリューションズ社
イノベーションセンター
Innovation Center, Connected Solutions Company


小林　正明　Masaaki Kobayashi
コネクティッドソリューションズ社
イノベーションセンター
Innovation Center, Connected Solutions Company
博士（工学）