＜基本計画書＞

IoT ワイヤレスセキュリティ通信における周波数有効利用技術に関する研究開発

１．目　的

全世界の IoT デバイスの数は、2015 年に約 158 億台であるが、2020 年には約 304 億台に達すると予測されているなど、IoT 時代には、通信ネットワークに接続される IoT ワイヤレスデバイスの急速な増加が見込まれている。これまでインターネット等のネットワークに接続していなかった機器が通信機能をもつことになり、多くの IoT 機器のマルウェア感染や乗っ取りが発生し、さらにその機器を悪用した DDoS 攻撃等の事例が多数発生している。また、HEMS 等の消費者向けサービスやコネクテッドカー等の自動車関連サービスに関連する IoT の脅威例も多数報告されている（※1）。加えて、国立研究開発法人情報通信研究機構（NICT）のサイバー攻撃観測・分析システム(NICTER)において、2015 年に観測されたサイバー攻撃 545 億件のうち、約４分の１が IoT デバイスを狙った攻撃であり、IoT ワイヤレスデバイスにおけるサイバーセキュリティ対策は、より一層求められる。そのため、IoT ワイヤレスデバイスのセキュリティを確保するために、今後、IoT ワイヤレスデバイスの機器認証や IoT ワイヤレスデバイスが扱うデータ認証が重要となるが、データ認証に係る通信トラフィックの増大によって周波数がひっ迫すると考えられている。

さらに、官公庁や企業等を狙った DDoS 攻撃等のサイバー攻撃のトラフィック量は年々増加している状況にあり、サイバーセキュリティ対策が十分には施されていない IoT ワイヤレスデバイスが DDoS 攻撃等の踏み台にされると、ワイヤレスネットワーク上に膨大な不正通信トラフィックが流れることも懸念されている（※2）。

このような状況を踏まえ、本研究開発では、認証プロトコルのメッセージのデータ量を削減する技術、認証のやり直し回数を削減する技術、暗号データのサイズを削減する技術、ワイヤレスネットワーク上における DDoS 攻撃等の不正な通信トラフィックを軽量な実装で検知して抑制することで周波数のひっ迫を抑止する技術等の確立を行い、周波数の有効利用に資することを目的とする。

※1　「IoT セキュリティガイドライン Ver1.0」
http://www.soumu.go.jp/main_content/000428393.pdf

※2　「CDNetworks Whitepaper　WP-9 2014 年 DDoS 攻撃の動向と今後の見通し」
http://www.cdnetworks.co.jp/data/whitepaper.html#wp-9

２．政策的位置付け

・サイバーセキュリティ戦略（平成 27 年９月４日 閣議決定）
５．目的達成のための施策
５．１ 経済社会の活力の向上及び持続的発展
５．１．１ 安全な IoT システムの創出
（４）IoT システムのセキュリティに係る研究開発・実証

「IoT システムの構成要素の特徴を加味した情報通信技術の開発・実証事業を行う」との記載あり。

・日本再興戦略 2016（平成 28 年６月２日 閣議決定）
第２ 具体的施策
Ⅰ 新たな有望成長市場の創出、ローカルアベノミクスの深化等
１．第４次産業革命の実現
（２）新たに講ずるべき具体的施策
ⅱ）第４次産業革命を支える環境整備
⑥サイバーセキュリティの確保と IT 利活用の徹底等
ア）サイバーセキュリティの確保
「官民を挙げた取組を進め IoT システム対策、研究開発、国際ルール等の形成等を強力に推進する。」との記載あり。

・電波政策 2020 懇談会 報告書（平成 28 年 7 月 15 日）
第３章 制度見直しの方向性
１．電波利用料の見直しに関する基本方針
（２）電波利用共益事務の在り方
②次期における電波利用料の使途
（オ）電波資源拡大のための研究開発、周波数ひっ迫対策のための技術試験事務
（ⅱ）IoT の社会展開に向けた電波有効利用技術の研究開発・実証
「IoT 無線機器に関し、セキュリティ上の脆弱性が原因で発生する大量かつ不要な電波輻射を抑制する技術や周波数のひっ迫を低減するための軽量暗号・認証技術等の研究開発も必要である。」との記載あり。

３．目 標

IoT 時代においては、IoT デバイスの普及によりワイヤレスネットワークへの接続デバイス数が増加するとともに機器認証のための通信トラフィックの増加が懸念されている。そこで、本研究開発では、IoT デバイスの使用が想定される周波数帯（700MHz 帯/800MHz 帯/900MHz 帯/1.5GHz 帯/1.7GHz 帯/2GHz 帯/2.4GHz 帯/5GHz 帯等）を対象とし、低消費電力であることが求められる膨大な数の IoT ワイヤレスデバイスの機器認証及びデータ認証時に効率的に通信する軽量認証技術を確立することにより、IoT ワイヤレスデバイスにおける同一周波数・時間での有効データ（通信データのうち、認証・暗号データを除いたアプリケーションデータ）量の 17%以上向上を目指す。あわせて、IoT ハブ（複数の IoT デバイスと接続しネットワークを介してクラウド上のサーバ等と送受信する装置）において、軽量な実装で、無線伝送の特徴を考慮したリアルタイムの帯域推定を行い、データの送信量を調整する技術を確立することで、現状としては送信されていないが追加で送信可能なデータ量の割合を削減し、同一周波数・時間での通信データ量を 1.5 倍以上に増加させることを目指す。

また、コスト上の問題により、IoT ワイヤレスデバイスが不正な通信を検知するた

めの十分なハードウェア能力を具備できないという課題がある一方で、IoT ワイヤレスデバイスが DDoS 攻撃等の踏み台となり多数の不正な通信が行われる懸念がある。そこで、軽量な実装により、IoT ワイヤレスデバイスの乗っ取りや詐称等による不正通信を 20 秒以内に検知・抑制することで、不正な通信の周波数占有率を低減し、同一周波数・時間での有効データ量の増加を目指す。

４．研究開発内容

（１）概要

本研究開発では、低消費電力であることが求められる IoT ワイヤレスデバイスの認証通信時のデータ量や回数を削減することやアプリケーションデータ通信時の暗号データサイズを削減する等の軽量認証技術、無線伝送の特徴を考慮したリアルタイムな帯域推定により送信データレートを制御する通信効率改善技術、ワイヤレスネットワーク経由で侵入してくる不正な通信（DDoS 攻撃等）を軽量な実装で検知し、抑制する不正通信検知・抑制技術を開発する。

（２）技術課題および到達目標

技術課題

ア）軽量認証技術/通信効率改善技術の開発

（ア-①）認証時通信データ量低減技術

IoT システムの認証については、認証にかかわる通信データ量が比較的大きく、ワイヤレスネットワークに流れる認証用データが大きいという問題がある。これに対して、TLS/DTLS(Transport Layer Security/Datagram Transport Layer Security)等の標準プロトコルを対象として､例えば認証プロトコルのメッセージのデータ量を削減するなどにより、ワイヤレスネットワークを流れるデータ量を削減する技術を開発する。この技術により、個々の IoT ワイヤレスデバイスの通信における認証通信部分の周波数占有率を低減し、空いた周波数部分を新たに活用可能となるため、同一周波数・時間での有効データ量の増加につながり、周波数利用効率の向上に資する。

（ア-②）認証回数低減技術

IoT ワイヤレスデバイスのメモリリソースが小さいと認証情報のメモリからの喪失により頻繁に認証（ハンドシェーク）のやり直しが必要となり、その都度、ワイヤレスネットワークに比較的大きな認証メッセージを流すことになる（通信データ量が大きくなる）という問題がある。これに対して、TLS/DTLS 等の標準プロトコルを対象として、例えば IoT ワイヤレスデバイスの認証情報の管理を最適化するなどにより、認証のやり直し回数を削減する技術を開発する。この技術により、個々の IoT ワイヤレスデバイスの通信における認証通信部分の周波数占有率を低減し、空いた周波数部分を新たに活用可能となるため、同一周波数・時間での有効データ量の増加につながり、周波数利用効率の向上に資する。

（ア-③）暗号付加データ量低減技術

暗号データに付加する情報が比較的大きいと、ワイヤレスネットワークに流れる暗号データも大きくなるという問題に対し、TLS/DTLS 等の標準プロトコルを対象として、例えば暗号データのサイズを削減する技術などを開発する。この技術により、個々の IoT ワイヤレスデバイスの通信におけるアプリケーション通信部分の周波数占有率を低減し、空いた周波数部分を新たに活用可能となるため、同一周波数・時間での有効データ量の増加につながり、周波数利用効率の向上に資する。

（ア-④）通信効率改善技術

IoT ワイヤレスデバイスの増加に伴い、認証や暗号化といったセキュリティ確保のための通信データ量が増大する傾向にあり、限られた周波数資源で効率的に伝送することが求められる。一般的に TCP/IP ネットワークでは、バーストトラフィックとの競合や、ネットワーク上でのパケット廃棄が過度なスループット減少を引き起こすため、周波数資源が空いていたとしても十分な送信データを出力できない現象が発生し、周波数資源を有効活用できないことが懸念される。

本問題を解消するためには、適切な送信データのスループットを推定する技術が必要であるが、ワイヤレスネットワークでは有線と異なり、電波環境の変動による帯域変化があり、有線と比較して適切な帯域推定が難しくなる。この問題に対して、IoT ワイヤレスデバイスから IoT サーバにデータを伝送する際、IoT ハブにおいて、軽量な実装でリアルタイムの帯域推定を実施し、どの程度のデータ伝送が可能な環境かを推定しながら、データの送信量を調整する技術を開発する。本技術により、バーストトラフィックとの競合等の条件下での帯域推定が原因で生じる、現状としては送信されていないが追加で送信可能なデータ量の割合を削減でき、同一周波数・時間での通信データ量を 1.5 倍以上に増加させることで、周波数の利用効率の向上に資する。

イ）不正通信検知・抑制技術の開発

IoT ワイヤレスデバイスから IoT ハブ、ワイヤレスネットワークを通して IoT システムのサーバにデータを伝送するシステムにおいて、IoT ワイヤレスデバイスが DDoS 攻撃等の踏み台となり不正な通信が行われること、並びに、IoT ハブが不正な通信を検知するために十分なハードウェア能力がコスト上の問題により具備できないという課題がある。例えば、ワイヤレスシステムとしてセルラシステムを活用する場合、各基地局に属する IoT ハブ、または同 IoT ハブに属する IoT ワイヤレスデバイスのいずれか１台でも DDoS 攻撃等の不正攻撃を受けると、断続的に基地局の周波数資源を消費し、他ユーザの利用を妨げることになる。また、同様の不正攻撃が首都圏内の基地局数千局で同時に発生すると、首都圏全体で正規利用サービスを妨害することになる。

本問題に対して、IoT ハブにおいて、軽量な実装で不正データ(DDoS 攻撃等)を検知し、ワイヤレスネットワークへの不正な通信を抑制する技術を開発する。こ

の技術により、不正な通信の周波数占有率を低減し、空いた周波数部分を新たに活用可能となるため、同一周波数・時間での有効データ量の増加につながり、周波数利用効率の向上に資する。

到達目標

ア）軽量認証技術/通信効率改善技術の開発

1 コネクションにおいて通信データ量の 50%を認証データが占めているとのデータがあり（※3)、(ア-①)（ア-②）（ア-③）で開発した技術により、例えば認証時の通信データ量や認証回数の削減および暗号化データ送信時の暗号付加データ量を削減し、同一周波数・時間での有効データ量の 17%*以上向上を目指す。

＊TLS/DTLSハンドシェークにおける証明書データや認証データ及びアプリケーション通信における暗号付加データのうち、削減が見込めるデータ量から目標値を設定。

※3 「The Cost of the “S” in HTTPS」
http://conferences2.sigcomm.org/co-next/2014/CoNEXT_papers/p133.pdf

またワイヤレスネットワークは有線と比較して電波環境および遮蔽物の有無等の構造物の地理的環境にも影響を受けやすく、スループット低下がどの程度あるか予測が難しいという問題がある。そこで（ア-④）で開発した、リアルタイムの帯域推定を実施し、データの送信量を調整する技術により、現状としては送信されていないが追加で送信可能なデータ量の割合を削減でき、同一周波数・時間での通信データ量を 1.5 倍*以上に改善することを目指す。

＊一般的にサーバ等の環境で適切な帯域推定を行った場合に得られる効果と同等程度の改善効果を、軽量な実装での IoT ハブにおいても出すことを目標として設定。

イ）不正通信検知・抑制技術の開発

IoT ハブを通過するパケット各々に対し、数多くの検知条件に合致しているかどうかをリアルタイムに判定することはハードウェア能力を必要とするため、攻撃に使われなくなった検知条件は破棄し、新たな攻撃を検知するための検知条件を取り入れることで、攻撃者の手法に合わせて少ない検知条件合致判定で効率的に攻撃を検知する技術が必要となる。これを実現するために、新たな攻撃検知条件を IoT ハブに反映、更新する手法により新規攻撃へも対応する。小リソースな IoT ハブに実装可能な軽量化技術により、IoT ワイヤレスデバイスの乗っ取りや詐称等による不正通信を 20 秒*以内に検知・抑制することで、不正な通信の周波数占有率を低減し、空いた周波数部分を新たに活用可能となるため、同一周波数・時間での有効データ量の増加につながり、周波数利用効率の向上に資する。

＊既存の有線通信で用いられている機器については、不正通信が大量に出た場合に 20 秒程度で検知・抑制するものが一般的であり、コンピュータリソースの少ない無線の IoT 機器の世界で実現することも加味して「20 秒」の目標値を設定。

なお、上記の目標を達成するに当たっての年度毎の目標については、以下の例を想定しているが、提案する研究計画に合わせて設定して良い。

（例）

＜平成２９年度＞

ア　軽量認証技術/通信効率改善技術の開発

・軽量認証技術の方式設計およびプロトタイプ開発を行う。

・通信効率改善技術の方式設計およびプロトタイプ開発を行う。

イ　不正通信検知・抑制技術の開発

・不正通信検知・抑制技術の方式設計およびプロトタイプ開発を行う。

＜平成３０年度＞

ア　軽量認証技術/通信効率改善技術の開発

・軽量認証技術のプロトタイプ評価を行う。

・通信効率改善技術のプロトタイプ評価を行う。

イ　不正通信検知・抑制技術の開発

・不正通信検知・抑制技術のプロトタイプ評価を行う。

＜平成３１年度＞

ア　軽量認証技術/通信効率改善技術の開発

・軽量認証技術の方式改良および評価（IoT ハブの仕様検証）を行う。

・通信効率改善技術の方式改良および評価（IoT ハブの仕様検証）を行う。

イ　不正通信検知・抑制技術の開発

・不正通信検知・抑制技術の方式改良および評価（IoT ハブの仕様検証）を行う。

５．実施期間

平成２９年度から平成３１年度までの３年間

６．その他

（１）成果の普及展開に向けた取組等

①国際標準化等への取組

国際競争力の強化を実現するためには、本研究開発の成果を研究期間中及び終了後、速やかに関連する国際標準化規格・機関・団体へ提案を実施することが重要である。このため、研究開発の進捗に合わせて、国際標準への提案活動を行うものとする。なお、提案を想定する国際標準規格・機関・団体及び具体的な標準化活動の計画を策定した上で、提案書に記載すること。

②実用化への取組

研究開発期間終了後も引き続き取り組む予定の「本研究開発で確立した技術の普及啓発活動」及び平成３６年度までの実用化・製品展開等を実現するために必要な取組を図ることとし、その活動計画・実施方策については、提案書に必ず具体的に記載すること。

③研究開発成果の情報発信

本研究開発で確立した技術の普及啓発活動を実施すると共に、総務省が別途指定する成果発表会等の場において研究開発の進捗状況や成果について説明等を行うこと。

（２）提案および研究開発に当たっての留意点

提案に当たっては、基本計画書に記されている目標に対する達成度を評価することが可能な具体的な評価項目を設定し、各評価項目に対して可能な限り数値目標を定めること。また、従来の技術との差異を明確にした上で、技術課題及び目標達成に向けた研究方法、実施計画及び年度目標について具体的かつ実効性のある提案を行うこと。

研究開発の実施に当たっては、関連する要素技術間の調整、成果の取りまとめ方等、研究開発全体の方針について幅広い観点から助言を頂くと共に、実際の研究開発の進め方について適宜指導を頂くため、学識経験者、有識者等を含んだ研究開発運営委員会等を開催する等、外部の学識経験者、有識者等を参画させること。

なお、本研究開発において実用的な成果を導出するための共同研究体制又は研究協力体制について、研究計画書の中にできるだけ具体的に記載すること。

また、４．（２）で開発した技術を統合実装した実証環境を構築し、開発した技術の有効性と実用化に向けた技術的課題を評価すること。その際、統合実証環境においても、４．（２）の到達目標を達成する性能を得ることを目標とすること。なお、統合実証環境は、実運用されている IoT ワイヤレスネットワークに近いシステム環境又は実用的な利活用シーンを想定したシステム環境とすること。