プレスリリース
報道関係　各位

2021 年 3 月 29 日
株式会社国際電気通信基礎技術研究所（ATR）
国立大学法人東北大学
エヌ・ティ・ティ・アドバンステクノロジ株式会社

無線通信への影響を極力抑える
高効率広域ネットワークスキャン技術を開発
～安心・安全な IoT 機器利用の実現に向けて～

株式会社国際電気通信基礎技術研究所(代表取締役社長:浅見　徹)、国立大学法人東北大学(総長:大野　英男)ならびにエヌ・ティ・ティ・アドバンステクノロジ株式会社（代表取締役社長：木村　丈治）は共同で、インターネット上に幅広く接続された機器のセキュリティ状態を把握するために必要となる、IoT[*1] 機器をはじめとした 1 億台以上のネットワーク機器に対してネットワークスキャン[*2] を効率的に実施できる技術を開発いたしました。

本技術はスキャン対象機器が接続されているネットワーク、特に有線ネットワークと比較して伝送速度の低い無線通信ネットワークにて行われている通信の品質劣化を極力引き起こすことなくネットワークスキャンを行えることが特長であり、IoT 機器などのセキュリティ状態の保全に役立てる技術となります。

開発した技術の一部については国際電気通信連合（ITU）および一般社団法人情報通信技術委員会(TTC) での勧告化・標準化も行いました。本研究は総務省電波資源拡大のための研究開発(JPJ000254)「周波数有効利用のための IoT ワイヤレス高効率広域ネットワークスキャン技術の研究開発」により実施したものです。

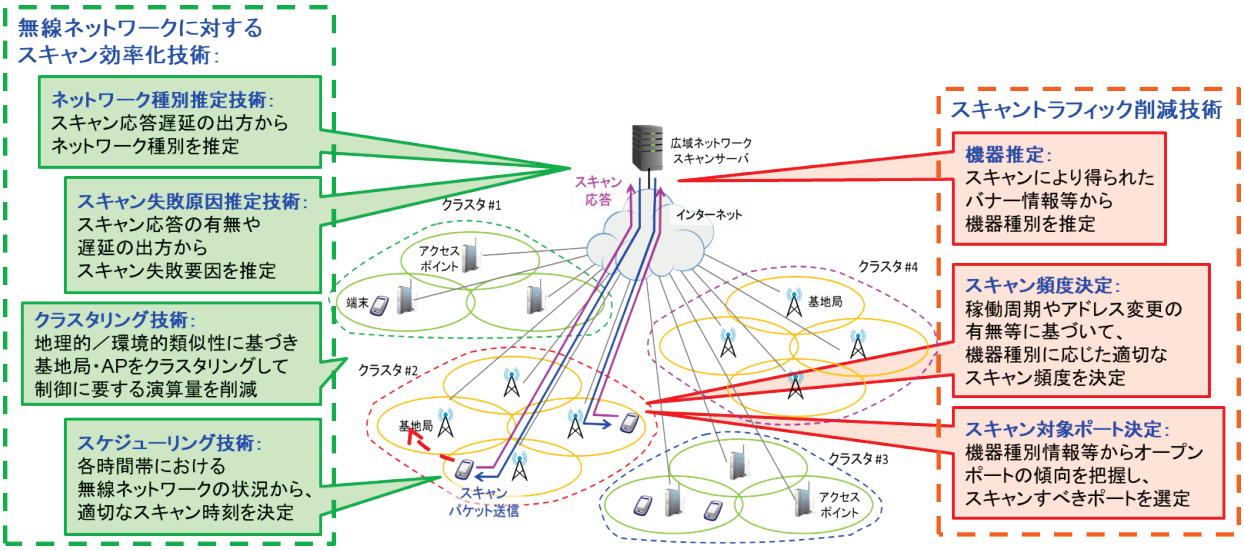


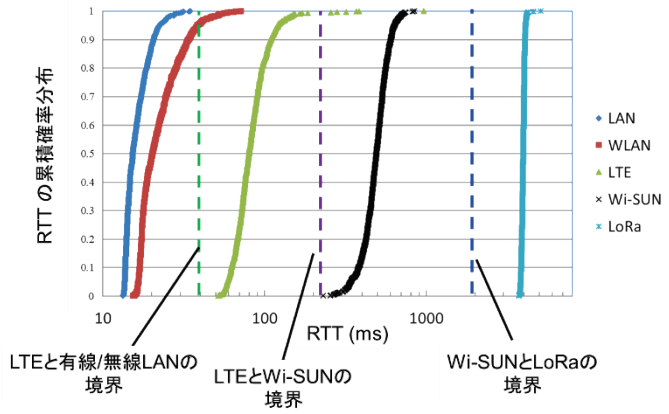
図-1　開発した高効率ネットワークスキャン技術のイメージ

● 無線通信ネットワークに対するスキャン効率化技術に関する取り組み

① ネットワーク種別推定技術

無線ネットワークには無線 LAN や携帯電話のような数 10 Mbps 以上の高速伝送が行えるものから、数 10～数 100 kbps 程度の伝送が行える IoT 通信向けの広域ネットワークである LPWA（Low Power, Wide Area）[*3] まで、通信速度が異なる様々なものが存在します。一度に実施可能なネットワークスキャンの量は通信速度に大きく依存するため、安定かつ効果的なネットワークスキャンを行いつつも（ネットワークスキャン以外の）通常の通信に与える影響を極力抑えるには、スキャン対象の機器がどのようなネットワークに接続されているかを知ることが非常に重要となります。

そこで、ネットワークスキャンを行ったときの応答遅延（Round Trip Time : RTT[*4]）を分析することでスキャン対象機器が接続されているネットワーク種別を推定する技術を開発しました。本技術はスキャン元からスキャン対象機器までのネットワーク段数と RTT から、スキャン対象機器が所属しているネットワーク内部の伝送遅延を推定し、それを図-2（左）に示すネットワーク種別境界の値と比較することにより、接続ネットワーク種別を推定します。4 種類の無線ネットワーク（無線 LAN、LTE（Long Time Evolution）[*5]、Wi-SUN[*6] および LoRa[*7]）について、スキャントラフィック以外の背景通信がある場合とない場合の双方についてテストベッドを用いて性能評価を行い、91%以上の確率で正しくネットワーク種別の推定ができることを確認いたしました（図-2（右））。



推定対象 NW	背景通信	推定結果			
		無線 LAN	LTE	Wi-SUN	LoRa
無線LAN	無し	98%	2%	0%	0%
	有り	97%	3%	0%	0%
LTE	無し	0%	100%	0%	0%
	有り	0%	100%	0%	0%
Wi-SUN	無し	0%	0%	100%	0%
	有り	0%	0%	91%	9%
LoRa	無し	0%	0%	0%	100%
	有り	0%	0%	0%	100%

図-2 （左）インターネット上で取得した 5 種類のネットワーク内の RTT 分布例
（右）開発技術によるネットワーク種別推定精度（青字：正答率、赤字：誤答率）

② スキャン結果・要因判別技術

無線 LAN では様々な要因によってスキャンが失敗したりスキャン応答の遅延が大きくなったりすることがあります。そこで、現在がスキャンを行うのに適した時間帯であるかどうかを判断するために、スキャンの応答結果から無線ネットワークがどのような状況にあるかを推定する方式を開発しました。例えば、無線 LAN では「ネットワーク混雑」「ネットワーク接続なし」「隠れ端末問題[*8]」「通信品質不足」「一部ポート閉塞」やネットワークへの接続・非接続が時々刻々変化する「不安定な端末」を推定対象とし、図-3 に示すように、端末毎、ポート毎のスキャンパケットの時系列遅延データを利用し、各遅延要因に特有の特徴によって分類することで、スキャン失敗・遅延の要因を推定します。また同技術についてテストベッドにおいて検証実験を行い、90%以上の確率で正しく要因を推定できることを確認しました。

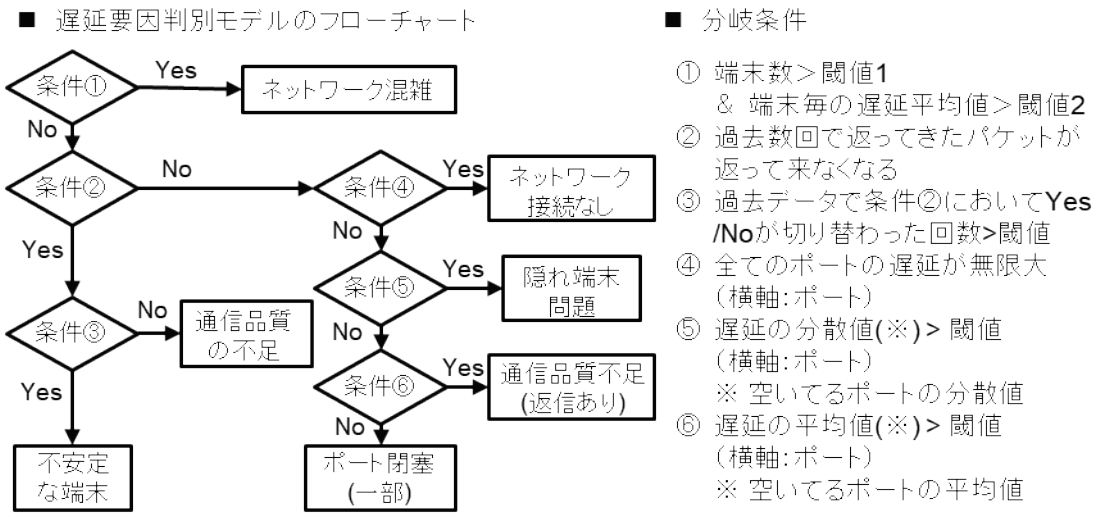


図-3　スキャン失敗・遅延要因判別の概要

③ クラスタリングを用いた計算量軽減技術

地理的近接性や無線環境が似ている複数の基地局やアクセスポイントをまとめてクラスタ化し、これらを単位としてスケジューリングを実施することで、スキャンを行うタイミングの制御(スケジューリング)に必要となる演算回数を削減する方式を開発しました。具体的には、1) ネットワークの混雑状況と無線区間におけるスキャンパケットの遅延時間の関係のモデル化、 2) スキャンパケットの遅延時間からスキャン以外の通信のスループットを推定する方法、 3) スキャン以外の通信の必要スループットを基にスキャンレートの最適値を導出する方法、を組み合わせて、最適なクラスタサイズを決定する技術を開発しました。この技術について数値解析を用いた検証実験を実施し、演算回数を大幅に低減可能であることを確認しました。

④ スキャンスケジューリング技術

スキャン対象のネットワークが混雑しているところにネットワークスキャンを実施するとネットワークの輻輳を引き起こし、スキャンの失敗やスキャン以外の通信の通信品質劣化が生じる問題があります。そこで、図-4 に示すように 1 日をいくつかの時間帯に分割し、各時間帯の混雑度をスキャン応答遅延から推定して、その結果に基づいて適切な時間帯にスキャンを行うスキャンスケジューリング技術を開発しました。テストベッドを用いた評価の結果、図-5 に示すように、開発技術はネットワークが混雑している時間帯を避けてスキャンを実施できており、ランダムなタイミングにスキャンのスケジューリングを行う場合と比較して、スキャン以外の通信の通信品質の劣化を小さく抑えられることを確認しました。

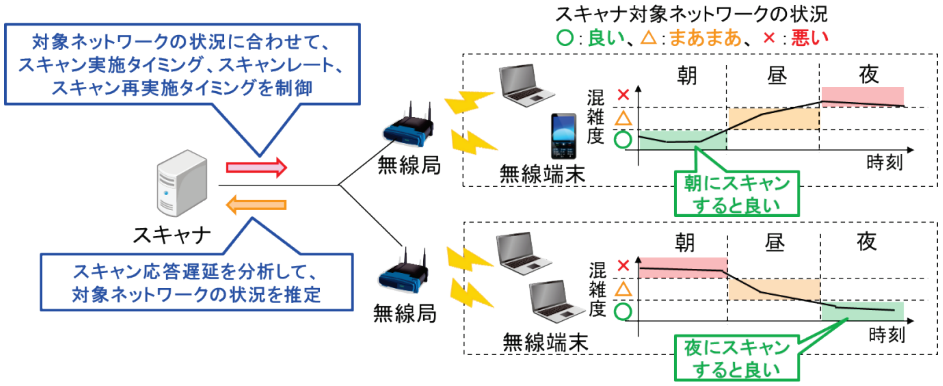


図-4　スキャンスケジューリングのイメージ

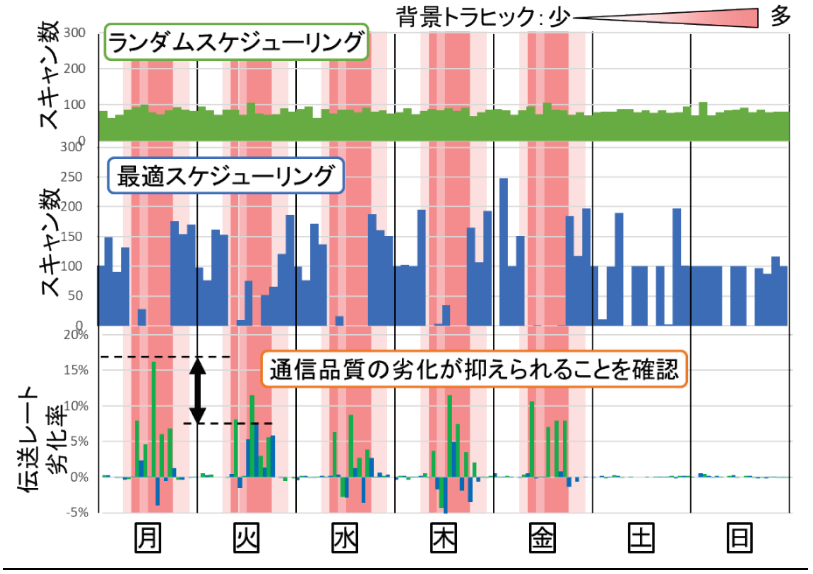


図-5　スキャンスケジューリングのテストベッドを用いた評価結果の例

● スキャントラフィック削減技術に関する取り組み

広域ネットワークスキャンを実施する場合、IoT 機器を含む多数の対象に対して TCP[*9] のフルポートである 65,535 ポートでスキャンを実施すると膨大なトラフィック量となり、既存のネットワーク通信等に悪影響を及ぼす可能性があります。そのため、通信量を抑えた効率的なスキャン方式が望まれています。そこでスキャンに係る通信量を削減する効率的なスキャン方式として、スキャン応答結果から IoT 機器を推定し、推定結果や応答特性に応じてスキャン対象ポートとスキャン頻度を最適化するスキャン方法を策定しました。

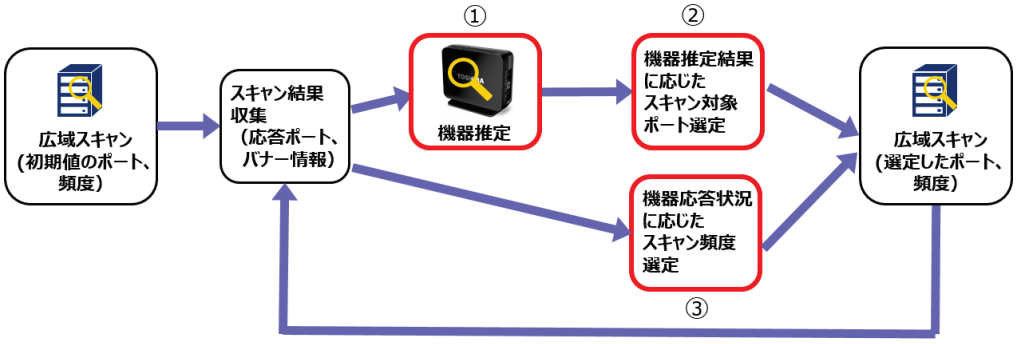


図-6　スキャンに係る通信量を削減する効率的な広域ネットワークスキャン方式

【標準的なスキャン方式】

提案方式と比較するために、まずは標準的なスキャン方式として、国内のインターネット応答状況を調査し、なるべく網羅的にスキャンが実施できるポートと頻度を定めたスキャン方式を策定しました。ランダムに選択した国内 1,000 万件の IP アドレスに対するフルポートスキャン、および応答のあった約 28 万件を対象とした 1 日 2 回のスキャンによる 2 週間の定点観測の結果から、ポートについては 1 つの IP アドレスから 100 以上のポート応答があるハニーポット[*10]等と想定されるものや、極少数（2 以下）の IP アドレスからしか応答がなかったポートを特異点として除外した約 11,700 ポート、頻度については応答の変更頻度の最小値 12 時間を Abuse[*11]等になりにくく、変化に追従できる最小頻度として設定しました。

【効率的なスキャン方式】

① 機器推定

機器推定はスキャンで得たバナー[*12]やポートを予め機器情報を登録した機器推定用データベースの情報と照合することにより行います。機器推定用データベースには、IoT 検索エンジン[*13]やセキュリティ事業者から入手した情報に加え、実際に広域ネットワークスキャンを実施して情報を収集した約 2,200 件の機器推定用データが登録されています。機器推定は、バナーとポートの類似度を算出することにより行います。バナー類似度は、スキャンにより取得したバナー情報とデータベースに格納されている各機器の重み付きキーワードとのマッチングを行い、算出します。一方、ポート類似度は、スキャンにより取得した応答ポート集合とデータベースに格納されている各機器の利用ポート集合を集合同士の類似度を表す Jaccard 係数[*14]により算出します。バナー類似度とポート類似度の加重平均により算出した機器類似度が、予め設定した基準点を超えた場合は機器が推定できたと判定し、その際にマッチングを行った機器を推定機器とします。

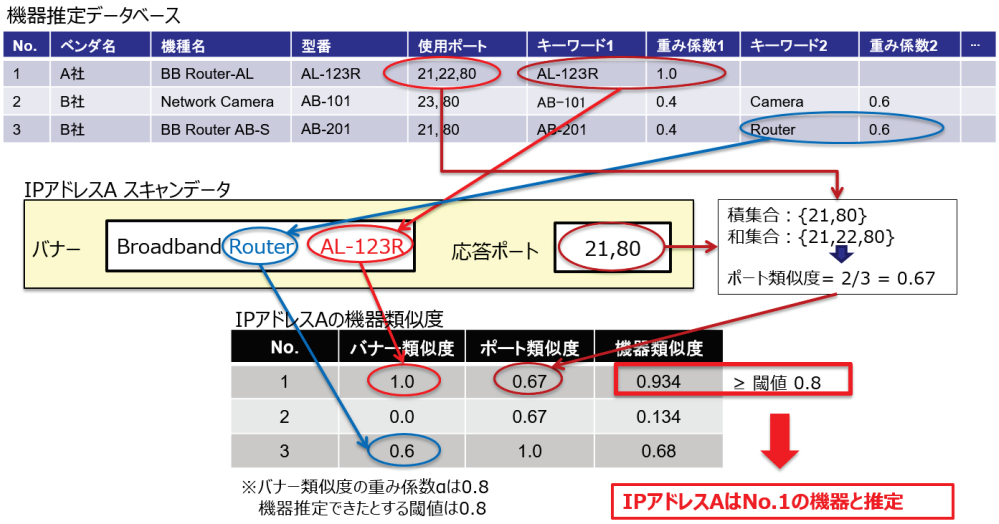


図-7　類似度算出による機器推定の実施例

② 最適なスキャン対象ポート

効率的なスキャン方式では、機器推定の可否によりスキャン対象ポートを変更して通信量を削減したスキャンを行います。何らかの応答がある IP アドレスに対して、機器が推定できた場合は当該機器が利用するポートでスキャンし、機器が推定できなかった場合は約 5,500 ポートでスキャンを行います。この約 5,500 のポートは、機器推定用データベー

スに登録された各 IoT 機器が利用するポート集合に加え、標準的なスキャン方式に比べて遜色ない検知となるように、標準的なスキャン方式で検出できるポートの 95%以上（ポート検出率 95%以上）を検出できるように応答の多いポートから順に足しこんで選定しました。また応答がない IP アドレスに対しては、今後新たに接続された機器を検知するため、標準的なスキャン方式で何らかの応答を検知できる IP 数に対して 95%の IP 数を検知できるポート数として、机上シミュレーションにより約 500 ポートでスキャンする設定としました。

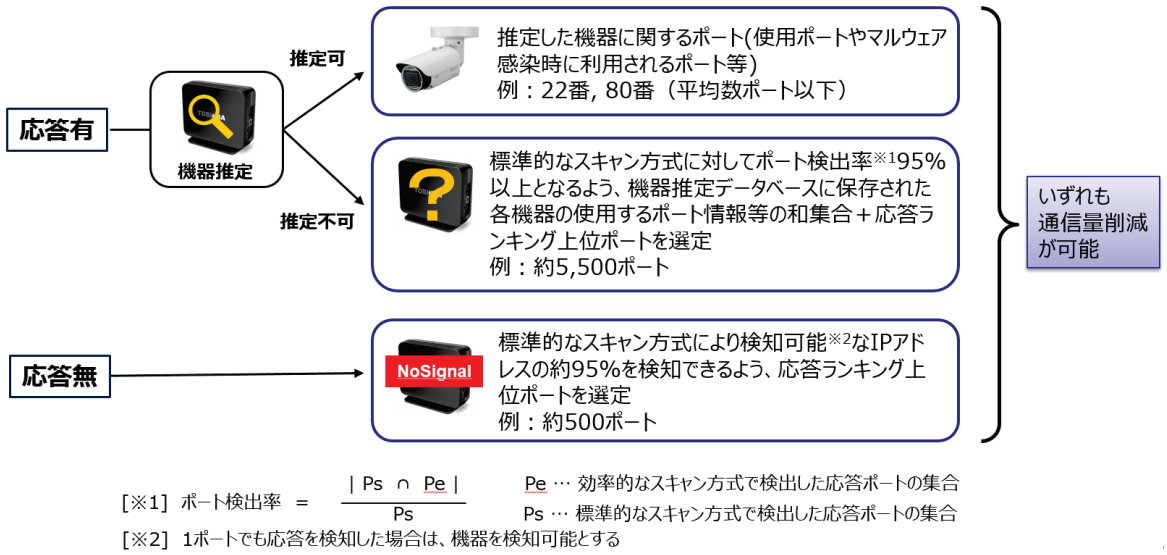


図-8　応答状況や機器推定結果に応じたスキャン対象ポートの選定

③ 最適なスキャン頻度

効率的なスキャン方式では、同じ IP アドレスから同じ応答が返ってきた場合は同じ機器が接続されていると推定し、スキャン頻度を少なくすることで通信量を削減します。具体的には、初期値の 12 時間から、1 日、2 日、3 日、5 日、7 日、14 日と徐々にスキャン間隔を延ばすことで頻度を少なくし、セキュリティ面も考慮して最長で 14 日に 1 回としました。前回から応答が変わった場合は機器が変更されたと推測し、スキャン間隔を初期値の 12 時間にリセットします。

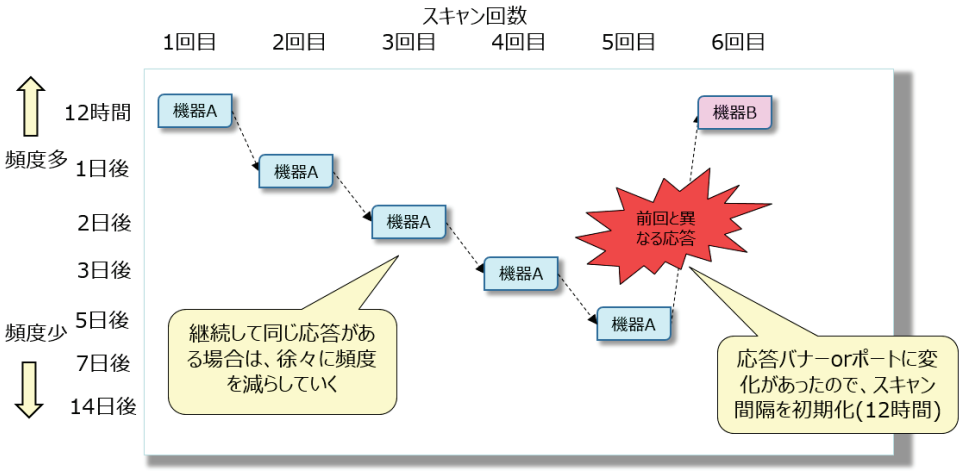


図-9　応答状況に応じたスキャン頻度の減少イメージ

● 統合評価

国内のインターネットからランダムに抽出した 10 万 IP アドレスを対象として、標準的なスキャン方式と効率的なスキャン方式の両方を用いた 4 週間の広域ネットワークスキャンを 2 回（対象 IP アドレスは異なる）実施し、スキャンに係る通信量とポート検出率の比較を行いました。また、その際の機器推定率（ただし、何らかのバナーを取得できたものが対象）も確認しました。結果から、通信量は標準的なスキャンに比べて約 1/38 と大幅な削減が可能となることを確認しました。また、その際のポート検出率は実インターネット上で行ったスキャン結果に基づくシミュレータでの評価で約 97.1%となり、標準的なスキャンに比べて大きく遜色がないことを確認しました。

● 開発した技術の標準化活動

ネットワークスキャンは見方を変えると「IP 接続性試験（インターネット上で試験対象機器に通信が正しくできるかどうかを確認する試験）の一種」と見なすことができます。そこで、開発した技術を広く社会に役立てる観点から、国際電気通信連合（ITU）内の通信分野の標準策定を担当する部門(ITU-T)において、開発した技術の標準化活動を行いました。具体的には、信号方式や試験方法の標準化を取り扱う ITU-T Study Group（SG）11 にて策定作業が進められていた勧告「Framework of IoT Testing」にネットワーク種別推定技術を含めることを提案し、2020 年 9 月に ITU-T 勧告 Q.4062 として成立しました。続いて、本勧告の内容について一般社団法人情報通信技術委員会(TTC)において国内標準制定の提案を行い、JT-Q4062「IoT 試験フレームワーク」として 2021 年 2 月に制定されました。

● 今後の展開

今後、本研究成果をより広く活用頂くために、効率的なスキャンツールや機器推定用データベースなどの学術研究機関等への提供、および製品化による販売等を検討しております。

＜用語・解説＞

*1) IoT（Internet of Things）：
身の回りの様々な物がインターネットに接続され、互いに情報交換を行うことで様々な制御を行えるようにする仕組み。

*2) ネットワークスキャン：
インターネットに接続されている機器に対してパケットを送出し、その応答の有無の確認や応答メッセージを取得する処理。

3*) LPWA（Low Power Wide Area）：
低消費電力で長距離の低速通信ができる IoT 向け無線通信技術の総称。

*4) RTT（Round Trip Time）：
メッセージを送信し、その応答が返ってくるまでの時間。

*5) LTE（Long Time Evolution）：
携帯電話の第 3.9 世代（3.9G）規格。第 4 世代（4G）と呼ばれる場合もある。

*6) Wi-SUN：
Wi-SUN Alliance が相互接続性認証を行っている、1 GHz 以下の周波数帯を使用する通信規格。
*7) LoRa：
LoRa Alliance が提唱する、1 GHz 以下の周波数帯を使用する LPWA の一種。
*8) 隠れ端末問題：
無線 LAN において、互いに相手の電波が届かない 2 台以上の無線局が同時に送信を行うことにより、受信局で衝突が発生して受信に失敗する問題。
*9) TCP（Transmission Control Protocol）
送り先にパケットが届いたかどうかを逐次確認し、届かない場合は再送や一度に送信するパケットの数を制御することで、送信パケットが可能な限り相手に届くようにする通信プロトコル。
*10) ハニーポット
不正アクセスの手法と傾向の調査を目的としてインターネット上に設置され、おとりとなって攻撃を受けて不正操作や不正通信のログを記録するシステム。
*11) Abuse
インターネット上の迷惑行為や不正行為。
*12) バナー
サービスが返すメッセージで、ソフトウェアや機器等の名称やバージョンが含まれる文字列。
*13) IoT 検索エンジン
インターネットに接続している IoT デバイスを検索可能な検索エンジン。SHODAN やミシガン大学の Censys が有名。
*14) Jaccard 係数
集合同士の類似度を表すもの。集合 A,集合 B の Jaccard 係数は、それぞれの積集合の要素数を和集合の要素数で割った値で示される。

【研究支援】
本技術は、総務省電波資源拡大のための研究開発（JPJ000254）「周波数有効利用のための IoT ワイヤレス高効率広域ネットワークスキャン技術の研究開発」によるものです。

■株式会社国際電気通信基礎技術研究所（ATR）について

本社：〒619-0288　京都府相楽郡精華町光台二丁目 2 番地 2（けいはんな学研都市）
代表者：代表取締役社長　浅見 徹
TEL：0774-95-1111
URL：https://www.atr.jp/
事業内容：脳情報科学、深層インタラクション科学、無線通信などの情報通信分野と生命科学に関する研究開発及び事業化

■国立大学法人東北大学について

本部所在地：〒980-8577　宮城県仙台市青葉区片平２丁目１－１
代表者：総長　大野 英男
URL：https://www.tohoku.ac.jp/japanese/
事業内容：研究・教育

■エヌ・ティ・ティ・アドバンステクノロジ株式会社について

本社：〒212-0014　神奈川県川崎市幸区大宮町 1310 ミューザ川崎セントラルタワー
代表者：代表取締役社長　木村 丈治
TEL：044-280-8811
URL：http://www.ntt-at.co.jp/
事業内容：システム/NW インテグレーション、関連ソフトウェア/サービス開発、セキュリティ関連サービス/製品販売、クラウド・IoT サービス/関連製品販売、RPA、NW・メディアアプリケーション関連の海外製品販売/保守、光関連製品開発、先端材料開発・分析、環境マネジメント、特許/商標など知的財産の調査分析等

【本件に関するお問い合わせ先】

■株式会社国際電気通信基礎技術研究所（ATR）
経営統括部　企画・広報チーム
TEL：0774-95-1176、FAX：0774-95-1178、Email：pr@atr.jp

■国立大学法人東北大学
大学院情報科学研究科　川本雄一
TEL：022-795-4287、FAX：022-795-4903、Email：youpsan@it.is.tohoku.ac.jp

■エヌ・ティ・ティ・アドバンステクノロジ株式会社
経営企画部 コーポレート・コミュニケーション部門　加藤・増田
TEL：044-280-8823、FAX：044-520-1530、Email：inquiry@ml.ntt-at.co.jp