TTCに寄せて

無線LANの標準化活動を振り返って
～TTC会長表彰を受賞して～

株式会社SRCソフトウェア
森岡　仁志

はじめに

このたびは「無線 LAN の標準化及び普及にかかわる功績」につきまして、大変名誉ある情報通信技術賞 TTC 会長表彰を賜り、光栄に存じます。また、これまで標準化作業においてご指導、ご協力いただいた皆様に深く感謝申し上げます。

私はルート株式会社（2011 年 株式会社アライドテレシス開発センターに吸収合併）に所属していた 2005 年より IEEE 802.11 WG に参加し、SRC Software（個人事業主）、株式会社 SRC ソフトウェアと独立後も参加を継続しています。その間、TGai（Fast Initial Authentication）や TGbc（Enhanced Broadcast Service）を立ち上げ、TGai では Secretary を、TGbc では Vice Chair を務めさせていただき、貴重な経験をさせていただきました。

本稿では私の IEEE 802.11 での活動を振り返り、IEEE 802.11 の標準化プロセスや IEEE 802.11ai、IEEE 802.11bc について紹介させていただきます。

IEEE 802.11 の標準化プロセス

IEEE（Institute of Electrical and Electronics Engineers）はアメリカに本部を置く学術研究団体で、その中に標準化を担う IEEE-SA（Standards Association）を持っています。IEEE 802.11 はその中で無線LANの標準化を行うグループとなります。IEEE 802.11 の中には TG（task Group）、SG（Study Group）、TIG（Topic Interest Group）、SC（Standing Committee）などがあり、IEEE 802.11xx の標準文書を作るのは TG になります。（図１参照）

IEEE 802.11 の運営ルールは明確に文書化されており、そのルールに従って標準化が進められます。決定事項は基本的に多数決で決められ、その多くは投票するための投票権が必要となります。投票権は年６回奇数月に開催される会合に最低３回出席することで得られます。投票権は個人に付与されるため、他の組織に移ってもその個人が保持することになります。

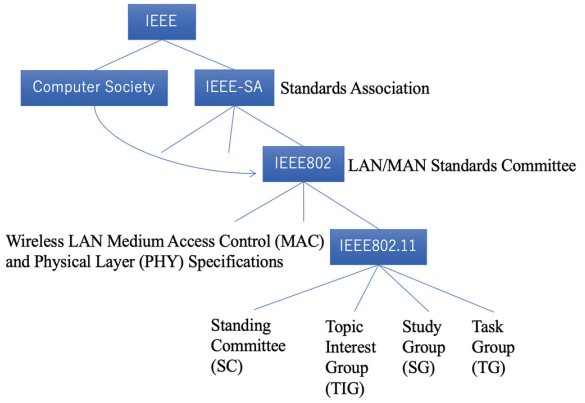

図１　IEEE 802.11 WG の構成

何か標準化したい技術がある場合、まず WNG SC（Wireless Next Generation SC）で提案を行い、賛同を集められれば SG または TIG が設立されます。TIG はそのトピックに関して標準化が必要かどうかを議論するグループで、標準化が必要となれば SG の設立を提案します。SG は TG を設立するための規定の文書である PAR（Project Authorization Request）と CSD（Criteria for Standards Development）を作成します。これらは、標準化の必要性・スコープなどを記述したもので IEEE 802.11 WG、IEEE 802 EC（Executive Committee）の承認を得て IEEE-SA に提出されます。IEEE-SA で承認されると TG が設立され、標準文書の作成が始まります。

TG では図２に示すように、技術提案を募り、多数決によって標準文書を作成します。ドラフトができると IEEE 802.11 WG で書面投票が行われ、得られたコメントに基づいてドラフトをアップデートするという作業を承認が得られるまで繰り返します。WG で承認されると IEEE-SA の希望者による SA Ballot が同様に行われ、SA Ballot で承認されると IEEE-SA の RevCom（Review Committee）に送付されます。

RevCom で承認されると出版され、標準化完了となります。

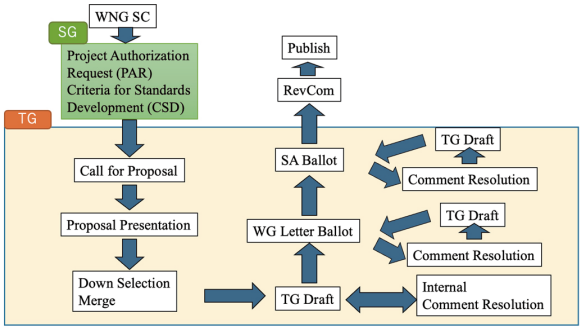

図2　IEEE 802.11 標準化の流れ

IEEE 802.11ai

初期の IEEE 802.11 で採用された認証・暗号化方式の WEP（Wired Equivalent Privacy）には深刻な脆弱性が発見され、後に IEEE 802.11i が制定されました。しかし、IEEE 802.11i ではアクセスポイント（AP, Authenticator）と端末（Supplicant）との間で 10 往復程度のパケット交換が必要となることが多く、一般に認証フレームは使用可能な最低送信レートで送信されるため、認証に時間がかかるだけではなく、CSMA/CA を使用する無線 LAN の仕様上、チャネルを長時間占有することにつながります。特に多くの人が利用する都心の駅などでは本来の目的であるデータ通信に利用できる帯域を圧迫してしまいます。そこで、私が当時所属していたモバイルインターネットサービス株式会社で独自の高速認証・接続プロトコルである MIS プロトコルを開発しました。

このプロトコルは端末－ AP －認証サーバ間の 1 往復のパケット交換で端末・AP・認証サーバの相互認証および鍵生成を完了するもので、前述の認証にかかる時間の短縮およびチャネル占有時間の短縮を実現しました。

また、実使用では IP を上位レイヤとして使用することがほとんどであり、IEEE 802.11 レイヤの接続だけではなく、IP アドレス・ゲートウェイアドレスなどの IP レイヤの設定も必要となります。一般には DHCP を使用して IP レイヤを設定しますが、これにも端末－ DHCP サーバ間で 2 往復のパケット交換が必要となります。そこで、MIS プロトコルでは認証パケットに IP レイヤの設定情報を含めることで、認証完了と同時に IP レイヤの設定も完了することができるようにしました。すなわち、MIS プロトコルでは端末－ AP －認証サーバ間の 1 往復のパケット交換で認証・鍵生成・IP レイヤ設定の全てを完了することができ、その後すぐにインターネットを使用可能となるようにしました。

この MIS プロトコルを標準にするべく、2005 年から IEEE 802.11 に参加を始め、当初は右も左もわからない状態で既存の TG で提案を行いましたが、案の定相手にされませんでした。

それからも参加を続け、2008 年に WNG SC でのある提案に対してコメントしたことがきっかけとなり、次の会合から WNG SC での提案を始めました。徐々に賛同者も増え、2010 年に SG の設立が承認され、2011 年より TGai として標準化作業が始まりました。

ちょうど IEEE 802.16（WiMAX）が一段落したのと重なったこともあり、各国の企業からたくさんの提案がなされ、2013 年に最初のドラフトが出来上がりました。それから書面投票とドラフトの修正を繰り返し、2016 年に標準化作業が完了し、IEEE 802.11ai として出版されました。

最初の提案から 8 年の歳月がかかり、私も途中で独立しましたが、様々な方のご協力により最後まで参加することができました。

ここで、IEEE 802.11ai の仕様を簡単にご紹介させていただきます。

無線 LAN に接続するには、まず接続先の AP を見つけ、接続（認証･鍵生成を含む）し、上位レイヤ（一般に IP レイヤ）の設定を行います。

IEEE 802.11 における AP の発見方法は 2 つあり、 1 つは AP が定期的に送信する Beacon を端末が受信するパッシブスキャンで、もう 1 つは端末が Probe Request を送信し、AP がそれに対して Probe Response を返信するアクティブスキャンです。パッシブスキャンでは端末は Beacon が送信されるのを待たなければならず、アクティブスキャンではチャネル占有時間が増えるという欠点があります。

IEEE 802.11ai では Beacon と次の Beacon の間に Beacon よりも小さいサイズの FILS Discovery Frame を送信することで端末の待ち時間を減らすことができるようにしました。また、Probe Response をブロードキャストできるようにし、アクティブスキャンにおけるチャネル占有時間を減らすようにしました。

認証・鍵生成については既存の Authentication および Association フレームを使用し、2 往復で完

了するようにしました。

IP レイヤの設定も既存の Association フレームを使用することで、１往復で完了するようにしました。

これにより、図３に示すように従来は多数のフレームが必要だった AP への接続が図４に示すように２往復で完了するようになりました。

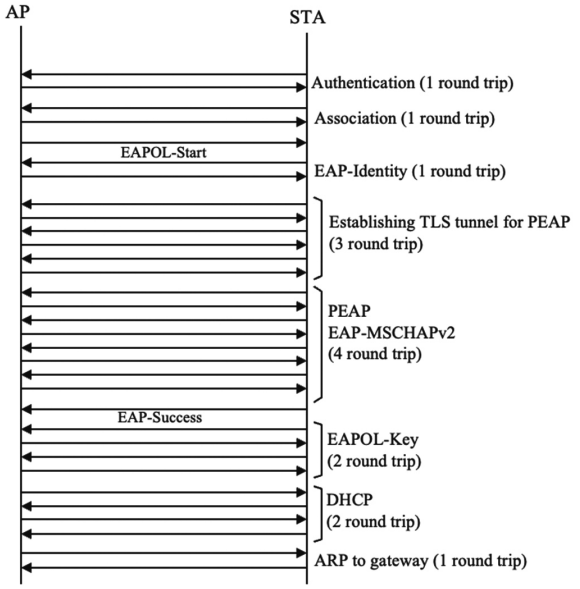

図３　従来の接続フレームシーケンス

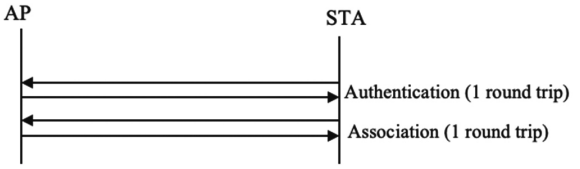

図４　IEEE 802.11ai による接続フレームシーケンス

IEEE 802.11bc

無線通信は電波の届く範囲にいれば受信できるため、放送に向いています。また無線 LAN は高速、免許不要、低コストであり、電波の到達距離も数十ｍ～数百ｍ程度とローカルな放送サービスに適しています。従来の IEEE 802.11 無線 LAN でもブロードキャストはサポートされていますが、アソシエーションを行なった端末のみを対象としています。１台の AP の最大アソシエーション数はプロトコル上 2007 台に制限され、また実際の運用上はパフォーマンスから数十台～数百台に制限されています。放送に特化すれば、アソシエーションは必要なく、AP が送信するデータを端末が受信するだけになるため、台数の制限も無くなります。また、端末は一切送信する必要がなくなるため、消費電力およびコストが削減されるだけでなく、プライバシーも容易に確保できるようになります。

放送型サービスを実現するには、偽送信者を排除するために送信されるデータの認証が必要となります。一方、受信者側は一切送信しない前提とするため認証鍵のネゴシエーションは行なえません。このような場合に使用できる認証方式に公開鍵暗号によるデジタル署名がありますが、デジタル署名は計算量が大きくなります。そのため、DoS 攻撃対策としてフレーム毎に認証することが望ましい一方、デジタル署名でのフレーム毎の認証は、動画などの大容量の配信を想定した場合、非力な受信端末では認証が追いつかなくなります。そこで、デジタル署名とハッシュチェーンを組み合わせる認証方式を考案しました。ハッシュチェーンとはハッシュ関数によってフレームの認証を行う方法です。

まず、送信者は図５に示すように乱数からハッシュ関数を使用して N+ １個の元鍵（K_i）および認証鍵（K'_i）を生成します。

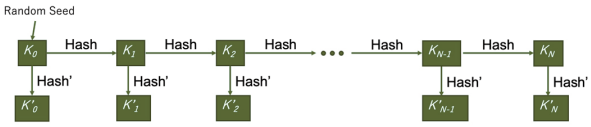

図５　ハッシュチェーン鍵生成

送信者は認証鍵を鍵とした HMAC ハッシュ関数を使用して各フレームの認証情報を生成します。図６に示すように、使用する認証鍵は生成時とは逆順に使用し、一定時間（T_K）で切り替えます。

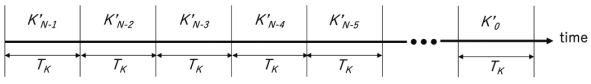

図６　認証鍵の使用

送信者は各フレームに認証情報を付加して送信し、図７に示すように $d * T_K$（$d \geqq 2$）後に元鍵を開示します。

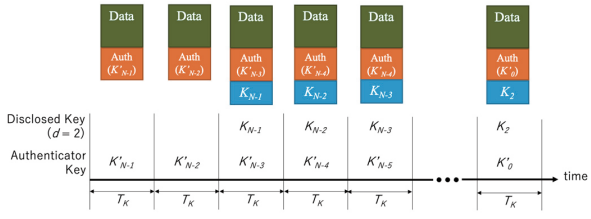

図７　元鍵の開示

受信者は元鍵が開示されるまでフレームをバッファし、元鍵が開示されると、まず元鍵の検証を行います。K_i+1 が検証済みで Hash（K_i）＝K_{i+1} であれば K_i は正しいと検証することができます。K_i が正しければ図８に示すように元鍵から Hash'（K_i）で認証鍵 K'_i を生成し、K'_i でフレームの認証情報を検証することでフレームを認証することができます。

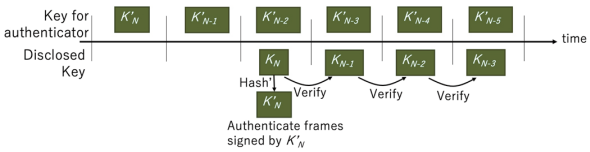

図８　フレーム認証

K_N の認証はハッシュで行えないため、この検証にはデジタル署名を使用します。K_N、デジタル署名、タイムスタンプなどの情報が含まれたフレームは EBCS Info フレームと呼び、図９に示すように T_K ＊ N の間隔で送信されます。

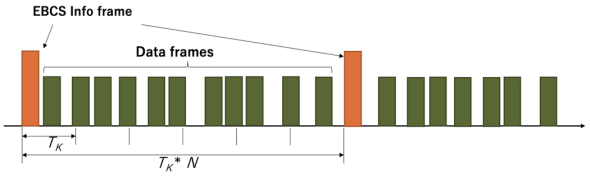

図９　フレームシーケンス

このように、デジタル署名とハッシュチェーンを組み合わせることで、フレーム毎の認証が可能となります。

これを標準化したいと思い、2017 年７月より WNG SC で提案を行い、2018 年１月に SG の設立が承認されました。2018 年 12 月に TGbc が設立され、技術提案を行うとともに副議長を務めました。この頃には顔見知りも多く、TGai のメンバーの参加もあり、割と気楽に進めることができました。ただ、コロナ禍で会合がキャンセルされたりオンラインのみになったりして、最初のドラフトができたのは 2020 年終盤になり、IEEE 802.11bc としての出版は今年２月になりました。

おわりに

IEEE 802.11 に参加して、技術的な勉強になったのはもちろんですが、民主的な議事の進め方など他にも多くのものを得ることができました。

IEEE 802.11 の参加者は増加傾向ですが、日本からの参加者は一時期に比べて減少気味です。一方、中国を中心に若手が大勢参加している企業もあります。ぜひ日本の企業からも若い方が参加していただければと思います。

最後になりましたが、これまでの標準化活動にご協力いただきました方々に改めて御礼申し上げます。