ブロードバンドアクセス、ワイヤレス接続、セキュリティを統合し、コネクテッドホームの5G FWA を最大限に活用する上で、主要な役割を果たす CPE

Thibaud Lepage
テクニカラー・コネクテッドホームの5G FWA 製品管理担当ディレクター

5G 固定無線アクセス（FWA）サービスの家庭への導入により、NSP と消費者の両者にとって大変有用な新しいブロードバンドオプションがもたらされることになります。ただし、長期的な成功を収めるには、NSP はブロードバンドアクセス、家庭内ワイヤレス接続、厳格なセキュリティ対策の3つを慎重に統合する必要があります。

キャリアクラスの5G FWA 用顧客構内設備（CPE）の設計、開発、展開に戦略的アプローチをとることによって、これらの3要因をどのように管理できるのでしょうか。それをより深く理解するために、テクニカラー・コネクテッドホームの5G FWA 製品管理担当ディレクターである Thibaud Lepage に話を聞きました。

以下にインタビューの内容をご紹介します。

5G 固定無線アクセス（FWA）は、未来のコネクテッドホームを考える上で重要な役割を果たします。消費者と NSP の両者にとってエキサイティングな時期となり、新世代の5G ホームゲートウェイは一部の市場に存在してきたテクノロジーのギャップを埋めるものと期待されています。というのも、これまで自宅内の完全なブロードバンド体験から取り残されてきた加入者にも、高速接続を提供できるようになるからです。NSP は現在、5G 固定無線接続を十分に活用する方法を模索しているところです。

しかし、それには慎重な対応が必要です。各家庭に5G FWA を供給するだけでは、家全体にブロードバンド接続を行き届かせ、複数のデバイスやユーザーにアクセスを提供するというメリットを活用することにはなりません。特定の1室に5G を供給することも重要ではありますが、高速ブロードバンドが家庭内のすべてのデバイスとユーザーに効果的に行き届かないのであれば、供給する意味がないのです。

高いパフォーマンスを維持していくためには、NSP はキャリアグレード品質のゲートウェイを導入する必要があります。テクニカラーのゲートウェイは、HOMEWARE および RDK-B テクノロジーに基づき、オープンシステムを活用しています。これが信頼性の高いマネージド型のミドルウェアを提供するための鍵となり、NSP はパートナー企業の活発なエコシステムを活用して、加入者に革新的なサービスを提供できるようになります。

テクニカラー・コネクテッドホームの HOMEWARE は、オープンな高付加価値の標準に基づいて開発されたもので、エンジニア達によって常にキャリアグレードに拡張されていま

す。RDK-B は、完全にカスタマイズ可能なオープンソースのソフトウェアソリューションであり、ブロードバンドを使用してコア機能を標準化します。このようなアプローチにより、消費者がスマートフォンにアプリを追加するのとほぼ同じ方法で、NSP もゲートウェイにアプリケーションを追加することができます。

テクニカラー・コネクテッドホームでは、HERO パートナープログラムを介してパートナー企業の開発したアプリを事前に統合し、アップグレードやメンテナンスなどを含めたサービスをすべてゲートウェイ内で改善しながら、アプリの完全なライフサイクル管理を提供できるようにしています。

たとえば、ゲートウェイは EasyMesh に対応しており、Airties や Plume とのパートナーシップによってコネクテッドホーム全体でシームレスな Wi-Fi ローミングを可能にしています。接続中のデバイスやユーザーの数は関係ありません。さらに、未来の真のコネクテッドホームを実現するために、さまざまな超高速の Wi-Fi リピーターとエクステンダーも揃えています。

セキュリティは最優先事項

過去2年間で、世界中の消費者は家庭内のネット接続にさらに依存するようになりました。これにより、膨大な量の機密データが生成され、デバイスやクラウドサービスの間で共有されています。つまり、セキュリティが最優先事項であることを意味します。

テクニカラー・コネクテッドホームの顧客構内設備（CPE）は、この優先順位を常に念頭に置いて設計されています。個人データ、プライバシー、ホームネットワークデバイスへのアクセスを著作権侵害やネットワーク攻撃から保護することは、当社の重要な責務です。

5G FWA 用 CPE も他の CPE も例外なく、ご家庭へのブロードバンド5G FWA アクセスを処理するための厳格なセキュリティ対策と併せて、ご家庭内のワイヤレス接続を可能にするデバイスへのハンドオフによる保護対策を講じています。これにより、NSP はエンターテインメントサービスから IoT デバイスまで、幅広いサービスを保護できるのです。テクニカラーでは、厳密な3段階のセキュリティチェックを採用して、デバイスミドルウェアとその上で実行されているアプリが適切に保護されていることを確認しています。

ステップ1：製品開発にコードのコントリビューションを受けるたびに、セキュリティの脆弱性がないか一晩かけて検証されます。バリデーション中も NSP に納品される前にも、開発者は自動的に通知を受け取ります。

ステップ2：コードは専任のセキュリティチームによって、オープンボックス（コードレビュー）とクローズドボックス（ペネトレーションテスト）の両方で総合的に検証されます。製品が納品された後も、専門チームがソフトウェアコンポーネントとテクノロジーを追跡し、継続的なセキュリティチェックとリスク評価を行います。独立したサードパーティのセキュリティ研究所でも、定期的に製品が検証されます。

ステップ3：最後に、実環境下で実際の運用中に製品のパフォーマンスが検証されます。テクニカラーでは、安全性、相互運用性、アプリ対応が確保された CPE 製品を提供するために、厳格なテストのための設備に投資しています。

テクニカラーが開発しているゲートウェイ専用のソフトウェア開発キット（SDK）により、NSP のお客様は新しいサービスを市場に投入し、統合型のソフトウェアアプリケーションを通じて加入者一人当たり売上高（ARPU）を向上させることができます。