Ellisys Expert Note | EEN_BT10
Rev. A

LE アイソクロナス通信の記録とセキュリティについて

tZERO™ Tracking Technology のメリット

はじめに

Bluetooth 5.2では、LE Power Control、Enhanced Attributes (EATT)、新しい LE アイソクロナスチャネルを介したBluetooth Low Energy上でのオーディオ伝送機能など、いくつかの主要な機能が導入されました。

このエキスパートノートでは、Bluetooth LEの物理チャネルの概念、2つの LE アイソクロナス転送の基本的な動作、これらの転送で使用されるセキュリティ、アクセス アドレスの使用方法などについて説明します。

また、Bluetooth LE で使用されるアイソクロナス通信の記録と暗号化・復号化に関してテスト機器が直面する課題と、これらの課題が Ellisys エンジニアリングチームによる独自のイノベーションによってどのように解決されたかを見ていきます。

Bluetooth LE 物理チャネル

Bluetooth LE 機器は、チャネルマップ（ホッピングシーケンスなど）、スロットタイミング、ランダム化されたアクセスアドレスなどの特性によって定義される共有物理チャネル上で通信します。

4種類のLE 物理チャネルでは、通信するペアの機器は、チャネルで定義された特性を用いて、同時に同じ PHYチャネルにトランシーバーを調整します。Bluetooth LE の4つの物理チャネルを**表1** に示します。

物理チャネル	目的
アイソクロナス	ピコネット内の接続された機器や未接続の機器の間で一定の間隔でアイソクロナスデータを転送（ブロードキャスト）
ピコネット	ピコネット内の特定の機器間通信に使用
アドバタイズ	デバイスへのアドバタイズメント配信に使用
ピリオディック（定期的アドバタイズ）	ユーザーデータを定期的にスキャナデバイスに送信

表1 Bluetooth Low Energy が使用する4つの物理チャネル

LEアイソクロナスチャネルは、いくつかの新しいプロファイルや、高性能で消費電力の少ない LC3 コーデックとともに、Bluetooth ユーザーに新しいオーディオ機能の提供を可能にしますが、これらは大きく分けて以下の二つのカテゴリになります。

- マルチストリームオーディオ（接続型）
- オーディオ共有のためのブロードキャスト（非接続型）

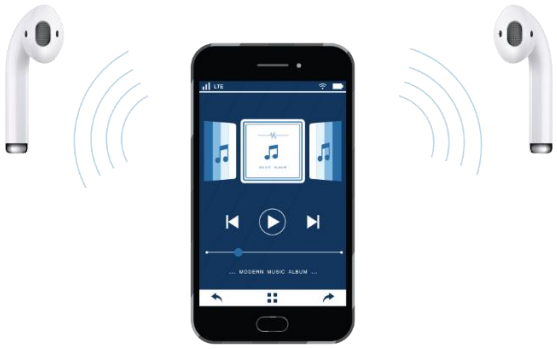


図1 マルチストリームオーディオがもたらす
真のワイヤレスステレオ体験

マルチストリームオーディオは、オーディオ発信器が同期している独立したオーディオストリームを送信し、そのオーディオを複数のオーディオ受信機で同時に鳴らすというものです。一方、従来の Bluetooth (BR/EDR) では、シングルストリーム方式を採用しており、これを中継することで TWS (True Wireless Stereo) を実現しています。

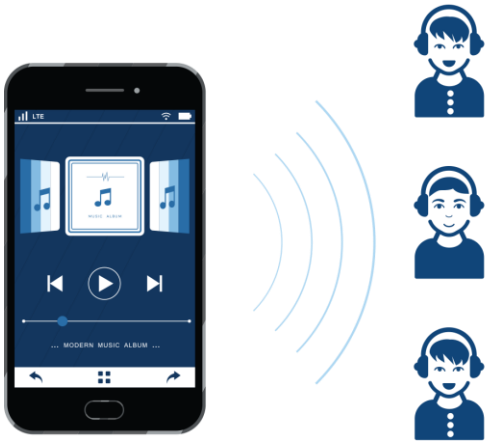


図2 ブロードキャスト オーディオ
パーソナルオーディオの共有例

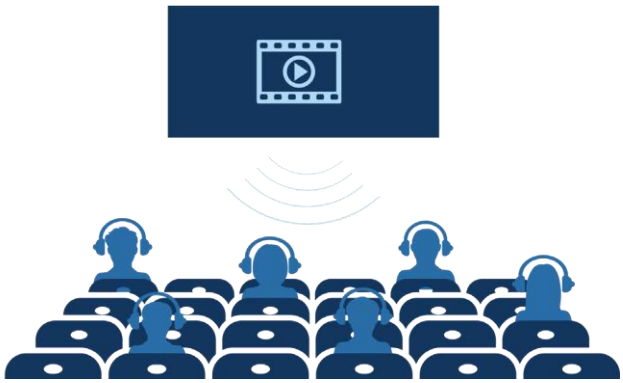


図3 公共の場に適したブロードキャスト オーディオ
位置情報を利用した音声共有の例

オーディオ共有機能は、1つのオーディオ発信機(アイソクロナスブロードキャスター)が、1つまたは複数のオーディオストリームを同期したオーディオ受信機にブロードキャストする機能です。

ヒント: Ellisys Bluetooth アナライザには、LC3 Auto-Detect 機能が搭載されています。これは Ellisys 独自の技術で、設定パラメータの記録なしでも LC3 コーデックに基づいて、LC3トラフィックを検出、デコードすることができます。

従来方式 （事前に設定パラメータの取得が必要）

LC3 自動検出

図4 LC3 自動検出

トランスポート	リンク
コネクテッド アイソクロナス ストリーム（CIS）	LE-S（ストリーム／アンフレームデータ） LE-F（フレームデータ）
ブロードキャスト アイソクロナス ストリーム（BIS）	LE-S（ストリーム／アンフレームデータ） LE-F（フレームデータ） LEB-C（放送制御）

表2 論理的トランスポートの種類

LE Audioのロジカルトランスポート

LE Audioの様々なアプリケーションに対応するために、2種類の論理トランスポートが定義されています。CIS は LE-ACL (Asynchronous Connection Logical) 接続で送られる LLCP コマンドで確立され、BIS はアドバタイズメント パケットで確立されます。

CIS は， 再送を促すために確認応答を使用し、データ対称またはデータ非対称（データは片方向または両方向に転送可能）とすることができます。1つの CIS は、1：1のセントラルデバイスと特定のペリフェラルデバイスで構成されます。

BIS には確認応答プロトコルがなく（受信者が応答しないため）、トラフィックは一方向にのみ送信され、1 ：多の同期した無制限の受信者に送信されます。しかし、BIS には無条件の再送メカニズムが組み込まれており、これを利用して信頼性を向上させることができます。CIS および BIS はそれぞれ、ISO_Intervals と呼ばれる一定の間隔で発生する「イベント」で構成されます。CIS および BIS のイベントは、1つまたは複数のサブイベントから構成されます。CIS サブイベントでは、セントラル およびペリフェラルデバイスがそれぞれ1回送信します。BIS サブイベントでは、ブロードキャスターは、アイソクロナスデータパケットを送信します。

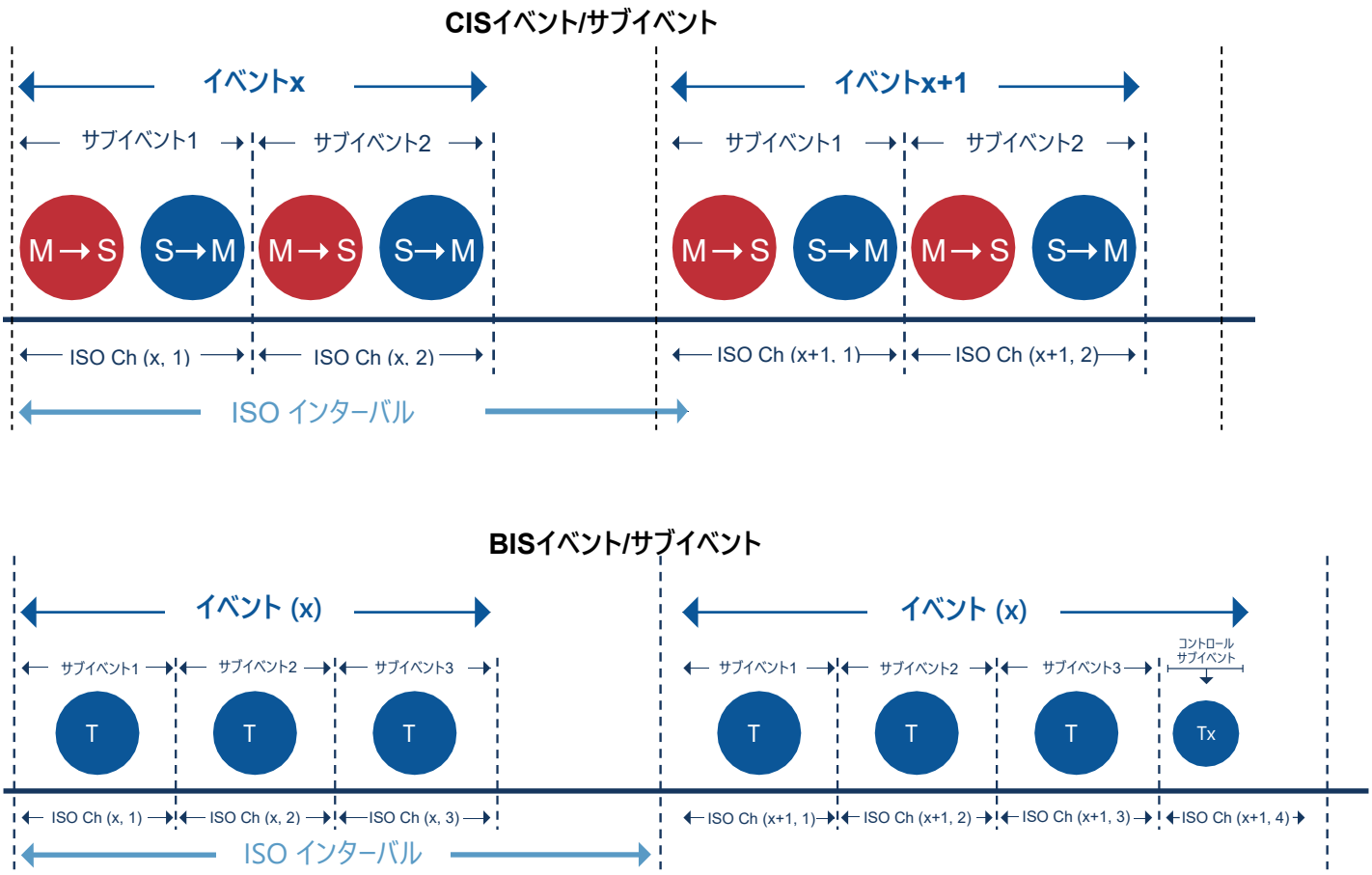


図5 CISとBISのイベントとサブイベント

接続されたアイソクロナスグループ (CIG) は、1つの CIS、または同じタイミング特性 (ISO Intervals) を持つ2つ以上の CIS で構成され、アプリケーション層との関係で最大31個のストリームが使えます。

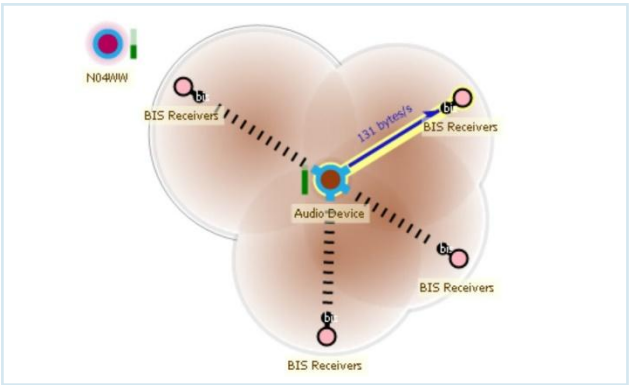


図6 アクティブなオーディオ PDU（および無関係なブロードキャスター）を含む4つの BIS ストリーム（1つの BIG）が表示された Instant Piconetビュー

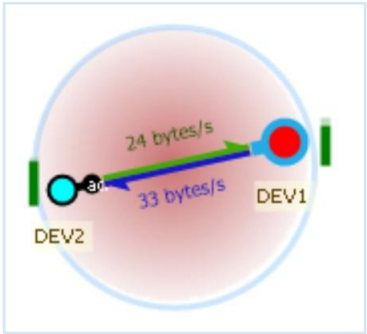


図7 単一の CIS (1:1のM-S 関係)
このケースでは、データが双方向に送受信

ブロードキャスターが作成するBIG (Broadcast Isochronous Group) には、1つまたは複数の BIS と、最大31個のストリームを含めることができます。CIS および BIS の主な機能を表3 にまとめました。

特徴	CIS	BIS
Ack 応答の必要性	はい	いいえ
データ転送	一方または双方向	一方向
再送	はい、Ack 応答で判断	はい、無条件で送信
ストリームまたはフレーム ロジカルリンク	両方	両方
コントロールロジカルリンク	LLCP（ACL）	LEB-C (ブロードキャスト制御)
ストリームの数	31 /グループ (CIG)	31/グループ (BIG)
ストリームトポロジー	１：１	１：多
PHY（1M、2M、 Coded S=2、S=8）	すべて	すべて
セキュリティ関連	ACL	BIG

表3 アイソクロナストランスポートの機能概要

LE アイソクロナス転送のセキュリティの基礎

ACL が暗号化されている場合、ACL で使用されるのと同じセッションキーを使用して、構成される CIS も暗号化されなければなりません。ACL が暗号化されていない場合、すべての構成される CIS は暗号化されません。BIG が暗号化されている場合、すべての構成される BIS は暗号化されなければなりませんが、空のPDUは暗号化されません。

BIG の暗号化と復号化には、いくつかのパラメータが必要です

BIG が暗号化されているかどうかを判断するために、リンク層は BIGInfo フィールドの長さをチェックします。暗号化されていない BIG の長さは 33オクテットで、暗号化された BIG の長さは 57オクテット（GIV + GSKD = 24 オクテット）です。

BIG への参加を希望するユーザーは、Broadcast Code (Privacy Code) を端末に入力する必要があります。Broadcast Code を用いて、Group Long Term Key (GLTK) を作成します。暗号化と復号化に使用される Group Session Key は、GLTK と GSKD から算出され、拡張アドバタイズメントパケット (AUX_SYNC_IND) の一部としてBIGInfo フィールドでブロードキャストされます。

パラメータ	長さ	ソース	備考
Broadcast Code	UI レベル: 最大16 オクテット、最小 4 オクテット その他のレベル： 128 ビット	ホストが提供	アプリケーション(UI) レベルで Bluetooth Privacy Code を呼び出し
Group Initialization Vector (GIV)	64 ビット	コントローラが生成し、AUX_SYNC_IND 内の BIGInfoフィールドを介して送信	Initialization Vector (IV) の計算に使用
Group Session Key Diversifier (GSKD)	128 ビット	コントローラが生成し、AUX_SYNC_IND 内の BIGInfoフィールドを介して送信	Group LTK と組み合わせて Group Session Key (GSK) を作成
Group Long Term Key (GLTK)	128 ビット	ホストが提供	Broadcast Code から作成

表4 BIGの暗号化パラメータ

ACLでは、接続が確立された時点で暗号化を開始することができます。暗号化は、CISにアクセスアドレスが割り当てられる前に有効となりますが、CISの暗号化および復号化にはアクセスアドレスが必要となるため、テスト機器にとっては複雑な作業となります。

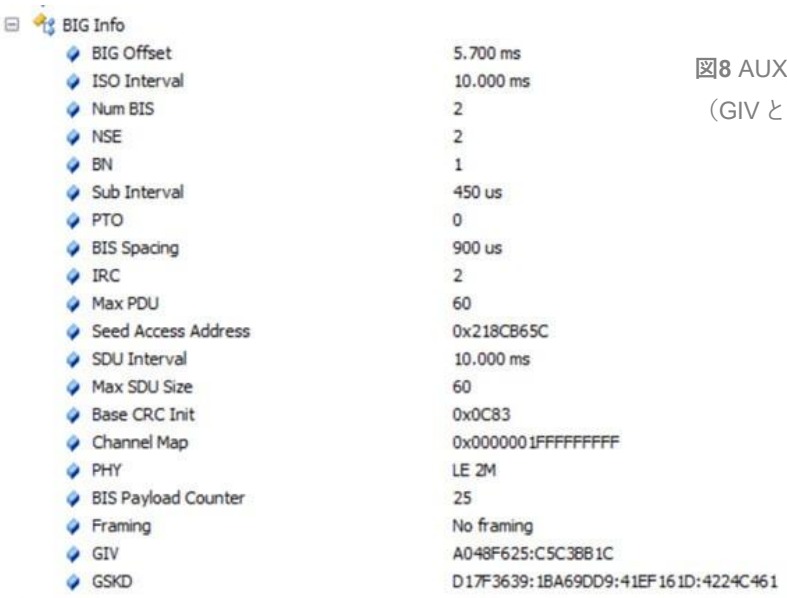


図8 AUX_SYNC_IND の BIGInfo フィールド（GIV と GSKD フィールドが存在する場合）

暗号化を実現するために、セントラルとペリフェラルの間でIV (Initialization Vector) とSKD (Session Key Diversifier) のパラメータが交換されます。これらの乱数はLL_ENC_REQ と LL_ENC_RSP PDU を用いて交換されます。各パラメータにはCentral 部とPeripheral 部があります。ACL の暗号化と復号化には、以下のようないくつかのパラメータが使用されます。

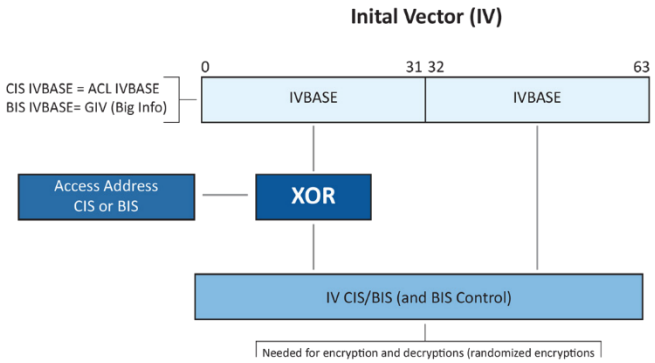
パラメータ	長さ	ソース	備考
Initialization Vector の Central 部 (IVm)	32 ビット	リンク層が生成し，LLCP 暗号化要求で送信	他の IV と連結して IV を作成
Initialization Vector の Peripheral 部 (IVs)	32 ビット	リンク層が生成し、LLCP 暗号化応答で送信	IVm と連結してIVを作成
Session Key Diversifier の Central 部 (SKDm)	64 ビット	リンク層が生成し，LLCP 暗号化要求で送信	SKDと連結してSKDを作成
Session Key Diversifier の \Peripheral 部 (SKDs)	64 ビット	リンク層が生成し、LLCP 暗号化応答で送信	SKDm と連結して SKDとする。

表5 ACLの暗号化パラメータ

Session Key Diversifierは、新しい接続ごとに新しいセッションキーを使用するために使われます。

Initialization Vectorは、Starting Variable (SV) と呼ばれることもあります。暗号化されたトラフィックをランダム化してパターンの繰り返しを防ぐための反復プロセスで使用されるビットのブロックで、平文の繰り返しから異なる暗号文を生成します。ランダム化とは、電子メールの署名や固定位置のヘッダーフィールドのように繰り返される平文があっても、同じ暗号文にならないようにすることで、攻撃者がトラフィックを復号化しにくくするという考え方です。

右の図9は、アクセス アドレス (CIS または BIS) が IV に直接入力される様子を示しています。IV は、アクセス アドレスと IVBASE を使用して作成されます。CIS の場合、IVBASE は関連 ACL の IV の値に設定され、BIS の場合、IVBASE は AUX_SYNC_IND の BIGInfo フィールドに含まれる GIV (Group IV) の値に設定されます。



アクセス アドレス

図9 CISとBISのIVの作成

前述の通り、アクセスアドレスは物理的なチャネルアクセスに使用されます。また、アクセスアドレスは、Bluetooth LE アイソクロナス転送のセキュリティにも重要な役割を果たします。**図10**では、アイソクロナスパケットの一部として、アクセスアドレスフィールドを示しています。アクセスアドレスフィールドは32ビットで、パケットのプリアンブルの後、ヘッダーの前にあります。

図10 ブロードキャスト パケットのアクセス アドレス フィールド

表6は、4種類の物理チャネルでアクセスアドレスがどのように生成されるかをまとめたものです。なお、アクセスアドレスをランダムにすると、アドレス可能な周期的アドバタイズやアクティブなピコネット デバイスが多く生成されます。

物理チャネル	アクセスアドレス生成
アイソクロナス	ランダムに生成されたもの（CIS、BIS）
ピコネット	ランダムに生成される
アドバタイズ	固定 (0x8E89BED6)
周期 (定期的なアドバタイズ)	ランダムに生成される

表6 アクセス アドレスの生成（ランダムまたは固定）

図11では、LLCP トラフィックのみを表示するフィルタを使用して、LLCP_CIS_IND交換が2回発生していることがわかります（色付き）。このケースでは暗号化が使用されており、LLCP Encryption Startの交換で確立されている。

デフォルトの ACL (AA = 0x364E99FB) では、2つのCIS ストリームが作成されています。

1. CIS1 AA = 0xEF14A8B1
2. CIS2 AA = 0x9F240CB3

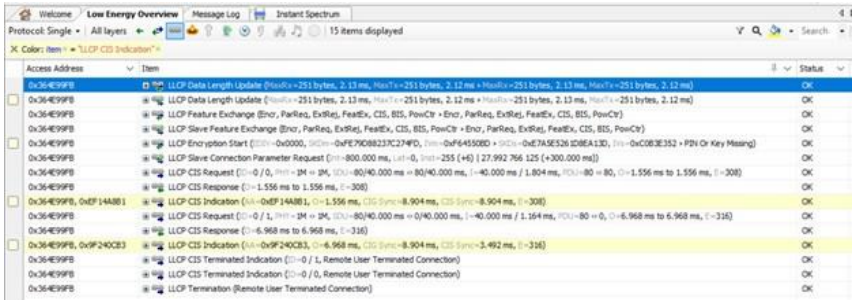


図11 ユニークでランダムなアクセスアドレスを持つ、2つの CIS を作成する ACL（ハイライト）

図12に，LLCP_CIS_IND パケットの内容を示します。このパケットには、CISのアクセスアドレスの他に、アイソクロナス転送を管理するための重要なパラメータが含まれています。

図12 LLCP CIS INDパケット

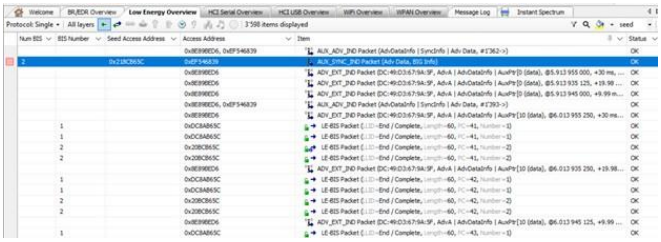


図13 BIG の Seed Access Address と2つの BIS Access Address を示すアドバタイズ シーケンス

図13では、アドバタイズパケット (0x8E89BED6 の固定値 AAを使用) が2つのBISを形成しています。AUX_SYNC_IND パケットの BIGInfoフィールドの NumBISの値は、2です。これらのストリームは、1つのBIGから作成されています。 BIG の Seed Access Address (SAA) は 0x218CB65C（AUX_SYNC_INDで提供）です。

これは、各 BIS のアクセスアドレスを作成するために使用されます。

1. BIS1 AA = 0xDC8AB65C
2. BIS2 AA = 0x20BCB65C

解析の課題を解決する tZERO Tracking Technology

ここでは、2つのアイソクロナス転送の基礎知識、物理チャネル、暗号化の基本、アクセスアドレスを確認した上で、テスト機器にとって LE アイソクロナス転送のセキュリティがどのように難しいか、また、tZERO Tracking Technology を搭載した Ellisys の解析システムを使用するエンジニアがどのようなメリットを得られるかを検証します。

CIS や BIS で伝送されたデータを復号化するには、いくつかの計算問題を解く必要があります。複雑なのは、リンクが暗号化されると、すぐにアイソクロナス転送が始まることです。このため、テスト機器による復号化は、最初のアイソクロナス転送を見逃さないように、ソフトウェアの介入なしに、非常に高速に行う必要があります。

さらに、多くの BIG が存在する場合もあります（公開テストイベント、多忙な検証ラボなど）。各 BIG には、多くの BIS（最大31個）が存在し、それぞれが固有のアクセスアドレスや、セキュリティ、データのタイミングに関する重要なデータを持っています。

CIS の場合、CIS アクセスアドレスを含む LLCP_CIS_INDパケット自体が暗号化されている場合があります。構成する CIS を復号化する前に、ACL を復号化する必要があります。

BIS を捕捉および復号するための課題は、BIG のパラメータを収集、保存、および分析システムで使用する必要があることです。前述のように、これらのパラメータは AUX_SYNC_IND パケットの BIGInfo フィールドで提供されます。これらのパラメータには、アクセスアドレス (Seed Access Address) を作成するための情報だけでなく、GIV や GSKD などの他の重要な情報も含まれています。

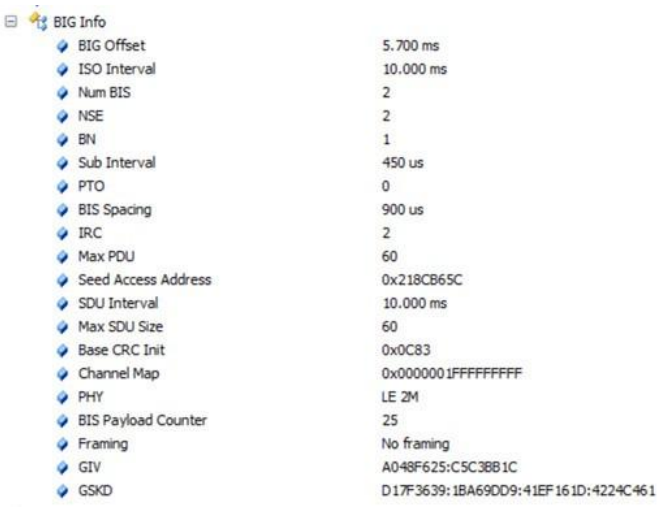


図**14** AUX_SYNC_IND パケットの Big Info フィールド

この他にも、コーデック、能力、機能など、解析装置が追跡すべき項目は数多くあります。解析装置は、これらの各領域に関連する様々なプロセスを管理しなければならず、これはハードウェアでは簡単に出来ません。解析装置のソフトウェアに負荷がかかり、時間がかかると、BIS 確立直後の BIS パケットの一部を見逃すことになります。
Ellisys の tZERO Tracking Technology は、アクティブな BIS をリアルタイムに追跡する方法を提供します。この技術では、すべての可能なアクセスアドレスをテーブルに読み込む必要がありません。パケットの取りこぼしや記録不可の時間はありません。

CIS の場合、CIS のアクセスアドレスが暗号化されたACL リンク層のパケットに含まれていることが課題となります。解析装置のハードウェアは、このアクセスアドレスが判明するまで、CISトラフィックの復号化を開始することができません。
ハードウェアのセキュリティキーだけに頼るのは限界があります。また、純粋な数任せの処理にも課題があります。CIG 内には複数の CIS が存在し、それぞれがアクセスアドレスやその他のコンテキスト情報を持ち、CIG も複数存在する可能性があります。

tZEROを使用しない場合、ACLトラフィックを復号化し、CIS/CIG の様々なパラメータを決定し、それをアナライザのハードウェアにフィードバックするために、時間のかかるソフトウェアの介入が必要となります。このトラフィックをライブで復号化するためには、アナライザソフトウェアは、記録を開始する前にリンクキーを知っていなければなりません。リンクキーなしで記録を開始した場合、CIS/CIG の接続を決定することができず、アナライザからは見えなくなります。
tZERO では、リンクキーがわからなくても、CIS の接続を実際に捕捉することができます。

まとめ

オーディオは、Bluetooth 技術の代表的なアプリケーションの一つです。BR/EDR (Classic Bluetooth) の実装がBluetooth オーディオ製品のかなりの部分を占めることは間違いありませんが、LE Audio によって可能になったアプリケーションを使用した新しい製品が登場しています。これらの新しいアプリケーションは、オーディオストリーミング、ブロードキャスト、オーディオ共有のコンセプトに基づいて構築されており、新しいコンシューマ製品、開発者のための新しいテスト要件、そして私たち全員が Bluetooth 技術をどのように使用するかについての新しいアプローチをもたらします。

Ellisys の中心となる理念は、開発者が可能な限り早く、最高の品質と性能を備えたツールを手に入れることです。また、拡張性があり、Bluetoothの仕様変更に対応できるツールを作ることも重要です。この理念のもと、Bluetooth 5.2とそれに伴う一連の新しいオーディオ機能の導入により、LE Audioのテストと開発の要件を満たすための新しい Bluetooth 解析製品を開発することになりました。Ellisys のエンジニアは、LC3 Auto-Detect と tZERO Tracking Technology を開発することで、世界中の無線技術アプリケーションに携わるエンジニアに選ばれてきた Ellisys 製品の革新的な精神を継承しています。

本文書について

本文書は、" EEN_BT10 Capture and Security Challenges Relating to the LE Isochronous Physical Channel (Rev. A - Updated 2021-09)" を翻訳したものです。原文、本文書及び Ellisys 製品に関するお問い合わせは、Ellisys 日本総代理店 ガイロジック株式会社 (0422-26-8211，es@gailogic.co.jp) までご連絡ください。
その他の翻訳版エキスパートノートは、https://www.gailogic.co.jp/db/bt/expert_notes をご覧ください。

Bluetoothプロトコル・アナライザ販売窓口　(ガイロジック株式会社)

0422-26-8211　**es@gailogic.co.jp**　**https://www.gailogic.co.jp/db/bt**