CHAPTER 1

LI の概要

この章では、Lawful Intercept（LI; 合法的傍受）について説明します。内容は次のとおりです。

注意 このマニュアルでは、LI の実装に関する法律上の義務については扱っていません。サービス プロバイダーには、自社のネットワークが、適用される LI の法規制に準拠していることを確認する責任があります。専門家に相談して、法律上の義務について確認することを推奨します。

LI の概要

LI とは、Law Enforcement Agency（LEA; 法執行機関）が、裁判所または行政の命令による権限に基づいて、個人（ターゲット）に対して電子的サーベイランスを実行するプロセスのことです。LI のプロセスを容易にするため、特定の法規制により、Service Provider（SP; サービス プロバイダー）および Internet Service Provider（ISP; インターネット サービス プロバイダー）は、認可された電子的サーベイランスを自社のネットワーク上で明示的にサポートすることが定められています。

このサーベイランスを実行するには、音声、データ、およびマルチサービス ネットワークの、従来の通信サービスおよびインターネット サービス上で通信傍受を行います。LEA は、ターゲットのサービス プロバイダーに対して通信傍受の要請を行います。サービス プロバイダーは個人に送受信されるデータ通信を傍受する責任があります。サービス プロバイダーは、ターゲットの IP アドレスから、ターゲットのトラフィック（データ通信）を処理しているエッジ Catalyst 6500 シリーズ スイッチを判別します。サービス プロバイダーは、ターゲットのトラフィックがこの Catalyst 6500 シリーズ スイッチを通過する際に傍受を行い、傍受したトラフィックのコピーをターゲットに知られることなく、LEA に送信します。

LI 機能は、米国内のサービス プロバイダーに求められる LI のサポート方法を定めた Communication Assistance for Law Enforcement Act（CALEA）に準拠しています。現在、LI は次の標準規格により定義されています。

- Telephone Industry Association（TIA）仕様 J-STD-025
- Packet Cable Electronic Surveillance Specification（PKT-SP-ESP-101-991229）

シスコの LI ソリューションの詳細については、シスコの代理店にお問い合わせください。

（注）　LI 機能は、音声とデータの傍受を含む CISCO-IP-TAB-MIB のオブジェクト citapStreamprotocol の定義に従って、IPv4 プロトコルの傍受をサポートします。

LI の利点

LI には、次の利点があります。

- 複数の LEA が、互いに知ることなく、同じターゲットに対して LI を実行できます。
- Catalyst 6500 シリーズ スイッチの加入者サービスに影響を与えません。
- 通信傍受を入力と出力の両方向でサポートします。
- レイヤ 1 およびレイヤ 3 トラフィックの通信傍受をサポートします。レイヤ 2 トラフィックは VLAN（仮想 LAN）上の IP トラフィックとしてサポートされます。
- 1 つの物理インターフェイスを共有する個々の加入者に対する通信傍受をサポートします。
- ターゲットは LI を検知できません。ネットワーク管理者も通話当事者も、パケットがコピーされていることや通話が傍受されていることに気付きません。
- SNMPv3（簡易ネットワーク管理プロトコル Verison 3）、および View-based Access Control Model（SNMP-VACM-MIB）や User-based Security Model（SNMP-USM-MIB）などのセキュリティ機能を使用して、LI の情報およびコンポーネントへのアクセスを制限できます。
- LI に関する情報へのアクセスを、最高特権を持つユーザだけに限定できます。管理者は、特権ユーザが LI 情報にアクセスできるように、アクセス権を設定する必要があります。
- 2 つのセキュリティ インターフェイスを使用して、傍受を実行できます。1 つは通信傍受を設定するインターフェイス、もう 1 つは傍受したトラフィックを LEA に送信するインターフェイスです。

CALEA for Voice

CALEA for Voice 機能により、VoIP 上で行われている音声通話の LI が可能です。Catalyst 6500 シリーズ スイッチは音声ゲートウェイ デバイスではありませんが、VoIP パケットは、サービス プロバイダーのネットワークのエッジにある Catalyst 6500 シリーズ スイッチを通過します。

認可された政府機関により通話が傍受の対象になると判断されると、CALEA for Voice 機能によりこの通話の IP パケットがコピーされて、詳しく分析するために、適切なモニタリング デバイスに送信されます。

LI に使用するネットワーク コンポーネント

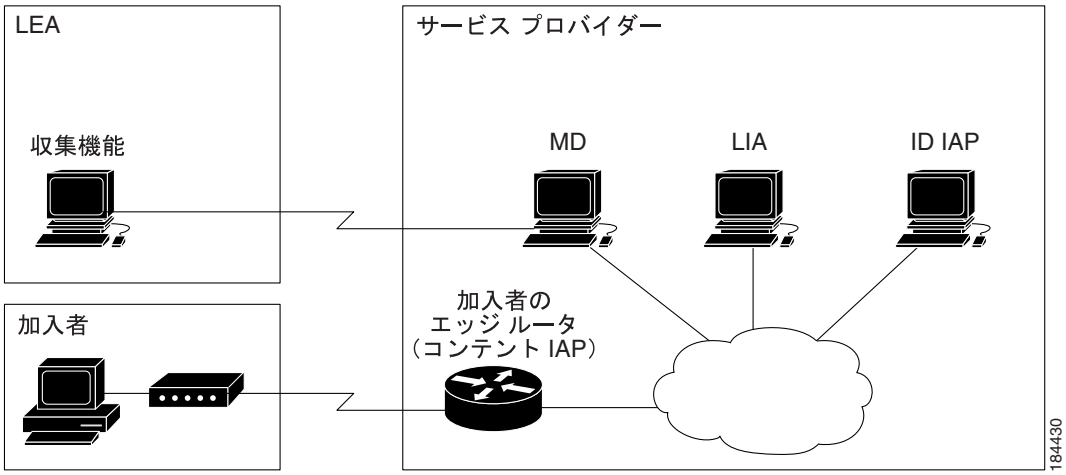
LI では、次のネットワーク コンポーネントを使用します。

- MD
- LIA
- IAP
- コンテント IAP

LI のプロセスについては、「LI のプロセス」（p.1-6）を参照してください。

図 1-1 に、LI モデルの概要を示します。

図 1-1　LI の概要



MD

LI のほとんどのプロセスは、Mediation Device（MD; メディエーション デバイス）（サードパーティ ベンダー製）によって処理されます。MD は、次の機能を実行します。

- LI の設定およびプロビジョニングのためのインターフェイスを提供します。
- 他のネットワーク デバイスに対して、LI の設定と実行を要求します。
- 傍受したトラフィックを LEA が要求する形式（国により異なる）に変換し、このトラフィックのコピーをターゲットに知られることなく LEA に送信します。

（注） 複数の LEA が同じターゲットを傍受している場合、MD は、傍受したトラフィックのコピーを LEA ごとに作成する必要があります。また、障害によって中断された LI を再開するのも MD の役割です。

LIA

Lawful Intercept Administration（LIA）は、LI または通信傍受の要求および管理のための認証インターフェイスを提供します。

IAP

Intercept Access Point（IAP）は、LI の情報を提供するデバイスです。IAP には、次の 2 種類があります。

- Identification（ID）IAP ― 傍受に必要な Intercept-Related Information（IRI; 傍受関連情報）（ターゲットのユーザ名、システム IP アドレスなど）、または VoIP に必要なコール エージェントを提供する Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバなどのデバイス。IRI の情報により、サービス プロバイダーはターゲットのトラフィックが通過するコンテント IAP（Catalyst 6500 シリーズ スイッチ）を特定します。
- コンテント IAP ― ターゲットのトラフィックが通過する、Catalyst 6500 シリーズ スイッチなどのデバイス。コンテント IAP には次の機能があります。
  - 裁判所の命令により指定された期間、ターゲットの送受信トラフィックを傍受します。Catalyst 6500 シリーズ スイッチは、宛先にトラフィックの転送を続けて、通信傍受が検知されないようにします。
  - 傍受したトラフィックのコピーを作成し、UDP パケットにカプセル化し、このパケットをターゲットに知られることなく MD に転送します。IP オプション ヘッダーはサポートされません。

（注）　コンテント IAP は、MD に、傍受したトラフィックのコピーを 1 つ送信します。複数の LEA が同じターゲットを傍受している場合、MD は、傍受したトラフィックのコピーを LEA ごとに作成する必要があります。

コンテント IAP

コンテント IAP は、対象となるデータ ストリームを傍受してコンテントを複製し、MD に送信します。MD は ID IAP およびコンテント IAP からデータを受信し、要求された形式（国により異なる）に変換して LEA に送信します。

LI のプロセス

LEA は、裁判所からサーベイランスを実行する命令または令状を取得したあと、ターゲットが加入しているサービス プロバイダーにサーベイランスを要請します。サービス プロバイダーの担当者は、MD で管理機能を実行して、（裁判所命令に従い）ターゲットの電子トラフィックを特定の期間モニタリングするために LI の設定を行います。

傍受を設定したあとは、ユーザが介入する必要はありません。管理機能が他のネットワーク デバイスと通信し、LI の設定を行って実行します。LI では、次の一連の処理が行われます。

1. 管理機能は ID IPA と通信し、ターゲットのユーザ名やシステム IP アドレスなどの IRI を取得し、ターゲットのトラフィックが通過するコンテント IAP（Catalyst 6500 シリーズ スイッチ）を特定します。
2. ターゲットのトラフィックを処理する Catalyst 6500 シリーズ スイッチが特定されると、管理機能により、その Catalyst 6500 シリーズ スイッチの MIB（管理情報ベース）に対して **get** および **set** 要求が送信され、LI が設定されてアクティブになります。CISCO-TAP2-MIB は、加入者ごとの傍受がサポートされている LI MIB です。
3. LI の間に、Catalyst 6500 シリーズ スイッチは次の機能を実行します。
   a. 着信および発信トラフィックを調べ、LI 要求の条件に一致するすべてのトラフィックを傍受します。
   b. 傍受したトラフィックのコピーが作成され、元のトラフィックはそのまま宛先に転送されるので、ターゲットに気付かれることはありません。
   c. 傍受したトラフィックを UDP パケットにカプセル化し、このパケットをターゲットに知られることなく MD に転送します。

（注） ターゲットのトラフィックの傍受および複製の処理によって、トラフィック ストリームに検知可能な遅れが生じることはありません。

4. MD は、この傍受したトラフィックを要求された形式に変換し、LEA で稼働している収集機能に送信します。傍受したトラフィックは、ここで格納され処理が行われます。

（注） 裁判所命令で許可されていないトラフィックを Catalyst 6500 シリーズ スイッチが傍受した場合は、MD により不要なトラフィックがフィルタリングされ、裁判所命令で許可されたトラフィックのみが LEA に送信されます。

5. LI の期間が終了すると、Catalyst 6500 シリーズ スイッチはターゲットのトラフィックの傍受を停止します。

LI MIB

LI を実行するために、Catalyst 6500 シリーズ スイッチは次の MIB を使用します。これらの MIB については、次のセクションで説明します。

- CISCO-TAP2-MIB — LI のプロセスに使用します。
- CISCO-IP-TAP-MIB — レイヤ 3（IPv4）トラフィックの傍受に使用します。

CISCO-TAP2-MIB

CISCO-TAP2-MIB には、Catalyst 6500 シリーズ スイッチ上の LI を制御する SNMP 管理オブジェクトが含まれています。MD はこの MIB を使用して、トラフィックが Catalyst 6500 シリーズ スイッチを通過するターゲットに対して LI を設定し、実行します。

CISCO-TAP2-MIB には、Catalyst 6500 シリーズ スイッチ上で実行される LI の情報を提供するための複数のテーブルが含まれています。

- cTap2MediationTable — 現時点で、Catalyst 6500 シリーズ スイッチ上で LI を実行している各 MD に関する情報が含まれています。テーブルの各エントリには、Catalyst 6500 シリーズ スイッチが MD と通信するための情報（デバイスのアドレス、傍受したトラフィックを送信するインターフェイス、傍受したトラフィックの転送に使用するプロトコルなど）が含まれています。
- cTap2StreamTable — 傍受するトラフィックを特定するための情報が含まれています。テーブルの各エントリには、LI のターゲットに関連するトラフィック ストリームを特定するための、フィルタへのポインタが含まれています。フィルタに一致するトラフィックが傍受され、コピーされて、対応する MD のアプリケーション（cTap2MediationContentId）に送信されます。

  cTap2StreamTable テーブルには、傍受したパケット数および傍受対象であっても傍受されなかった廃棄パケット数のカウントも含まれています。
- cTap2DebugTable — LI のエラーをトラブルシューティングするためのデバッグ情報が含まれています。

CISCO-TAP2-MIB には、LI イベントに関する SNMP 通知も含まれています。MIB オブジェクトの詳細な説明については、MIB を参照してください。

CISCO-TAP2-MIB のプロセス

管理機能（MD 上で実行）により、Catalyst 6500 シリーズ スイッチの CISCO-TAP2-MIB に対し SNMPv3 の **set** および **get** 要求が発行され、LI が設定および開始されます。具体的には、次の処理が行われます。

1. cTap2MediationTable のエントリを作成し、Catalyst 6500 シリーズ スイッチと傍受を実行する MD との通信方法を定義します。

   （注）　cTap2MediationNewIndex オブジェクトは、メディエーション テーブル エントリの固有のインデックスです。

2. cTap2StreamTable にエントリを作成し、傍受するトラフィック ストリームを特定します。
3. cTap2StreamInterceptEnable を true(1) に設定して、傍受を開始します。Catalyst 6500 シリーズ スイッチは、傍受期間（cTap2MediationTimeout）が終了するまでストリーム内のトラフィックを傍受します。

CISCO-IP-TAP-MIB

CISCO-IP-TAP-MIB には、Catalyst 6500 シリーズ スイッチを通過する IPv4 トラフィック ストリームに対して LI を設定および実行するための SNMP 管理オブジェクトが含まれています。この MIB は CISCO-TAP2-MIB の拡張版です。

CISCO-IP-TAP-MIB を使用して Catalyst 6500 シリーズ スイッチに LI を設定し、次の 1 つまたは複数のフィールドの値と一致する IPv4 パケットを傍受できます。

- 宛先 IP アドレスおよびマスク
- 宛先ポート範囲
- 発信元 IP アドレスおよびマスク
- 発信元ポート範囲
- プロトコル ID

CISCO-IP-TAP-MIB のプロセス

データを傍受する場合は 2 つのストリームが作成されます。1 つは、任意のポートを使用してターゲット IP アドレスから任意の IP アドレスに発信されるパケットのストリームです。もう 1 つは、任意のポートを使用して任意のアドレスからターゲット IP アドレスにルーティングされるパケットのストリームです。VoIP の場合も 2 つのストリームが作成されます。1 つは、ターゲットからの RTP パケットのストリームです。もう 1 つは、特定の発信および宛先 IP アドレスとポートからターゲットに向かう RTP パケットのストリームで、IP アドレスとポートは RTP ストリームのセットアップに使用する SDP 情報で指定します。