CHAPTER 1

合法的傍受の概要

この章では、Lawful Intercept（LI; 合法的傍受）の情報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、合法的傍受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、適用される合法的傍受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。

合法的傍受の概要

合法的傍受とは、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。合法的傍受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 アドレスまたはセッションから、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 ルータを判別します。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ルータ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。

合法的傍受機能は、米国内のサービス プロバイダーに求められる合法的傍受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、合法的傍受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）

シスコの合法的傍受ソリューションの詳細については、シスコのアカウント担当者にお問い合わせください。

合法的傍受の利点

合法的傍受には、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合法的傍受を実行できます。
- ルータ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 3 およびレイヤ 2 トラフィックの通信傍受をサポートします。
- 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。
- ターゲットは合法的傍受を検知できません。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づきません。
- 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、合法的傍受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。
- 合法的傍受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、特権ユーザが合法的傍受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合法的傍受が可能です。Cisco 7600 シリーズ ルータ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ルータを通過します。

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。

合法的傍受に使用するネットワーク コンポーネント

合法的傍受では、次のネットワーク コンポーネントを使用します。

- MD
- IAP
- 収集機能

合法的傍受のプロセスについては、「合法的傍受のプロセス」（p.1-4）を参照してください。

MD

合法的傍受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。

- 合法的傍受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、合法的傍受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合法的傍受を再開するのも MD の役割です。

IAP

Intercept Access Point（IAP）は、合法的傍受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）を提供する Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）サーバなどのデバイス。サービス プロバイダーは、IRI の情報により、ターゲットのトラフィックが通過するコンテント IAP（ルータ）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、Cisco 7600 シリーズ ルータなどのデバイス。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。ルータは、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、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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）　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。

収集機能

収集機能は、サービス プロバイダーによって傍受されたトラフィックの格納と処理を行うプログラムです。このプログラムは、LEA にある機器上で動作します。

合法的傍受のプロセス

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、（裁判所の命令に従い）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合法的傍受の設定を行います。

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、合法的傍受の設定を行って実行します。合法的傍受では、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（ルータ）を特定します。
2. ターゲットのトラフィックを処理するルータが特定されると、管理機能により、そのルータの MIB に対して **get** および **set** 要求が発行され、合法的傍受が設定されてアクティブになります。合法的傍受の MIB には、CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB、および CISCO-USER-CONNECTION-TAP-MIB（加入者単位の傍受がサポートされている場合）が含まれます。
3. 合法的傍受の間に、ルータ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、合法的傍受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）　裁判所の命令で許可されていないトラフィックをルータが傍受した場合は、MD により不要なトラフィックがフィルタリングされ、裁判所の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. 合法的傍受の期間が終了すると、ルータはターゲットのトラフィックの傍受を停止します。

合法的傍受の MIB

合法的傍受を実行するために、ルータは次の 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 — 合法的傍受の処理に使用します。
- 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-802-TAP-MIB — レイヤ 2 トラフィックの傍受に使用します。
- CISCO-USER-CONNECTION-TAP-MIB — 個々の加入者のトラフィックの傍受に使用します。

CISCO-TAP2-MIB

CISCO-TAP2-MIB には、ルータ上の合法的傍受を制御する 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、トラフィックがルータを通過するターゲットに対して、合法的傍受の設定を行って実行します。この MIB は、合法的傍受をサポートするシスコのソフトウェア イメージにバンドルされています。

CISCO-TAP2-MIB には、ルータ上で実行される合法的傍受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、ルータ上で合法的傍受を実行している各 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、ルータが 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、合法的傍受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。

  このテーブルには、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 — 合法的傍受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、合法的傍受イベントに関する 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、ルータの CISCO-TAP2-MIB に対し SNMPv3 の **set** および **get** 要求が発行され、合法的傍受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、ルータおよび傍受を実行する 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。ルータは、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、ルータを通過する IPv4 トラフィック ストリームに対して合法的傍受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-802-TAP-MIB

CISCO-802-TAP-MIB には、ルータを通過する IEEE 802 データ ストリームに対して合法的傍受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。

CISCO-USER-CONNECTION-TAP-MIB

CISCO-USER-CONNECTION-TAP-MIB には、ルータ上の個々のユーザ接続（セッション）に対して通信傍受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 には、ユーザ接続に関する情報が含まれています。各接続は、一意のセッション ID で識別されます。