合法的傍受 2.0

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 *1* : 機能の履歴

機能名	リリース情報	説明
合法的傍受 2.0	Cisco vManage リリース 20.9.1	これは、合法的傍受バージョン 2.0 を導入する機能です。合法的傍受 2.0 の機能では、マネージド サービス プロバイダー（MSP）によってキャプチャされた Cisco Catalyst SD-WAN IPsec トラフィックを復号できるように、キー情報が Cisco Catalyst SD-WAN ルータおよび制御コンポーネント によって法執行機関（LEA）に提供されます。これは、LEA が暗号化されたネットワークトラフィック情報を復号するのに役立ちます。合法的傍受 1.0 の詳細については、Cisco Catalyst SD-WAN の『ポリシー設定ガイド』の「合法的傍受」の章を参照してください。

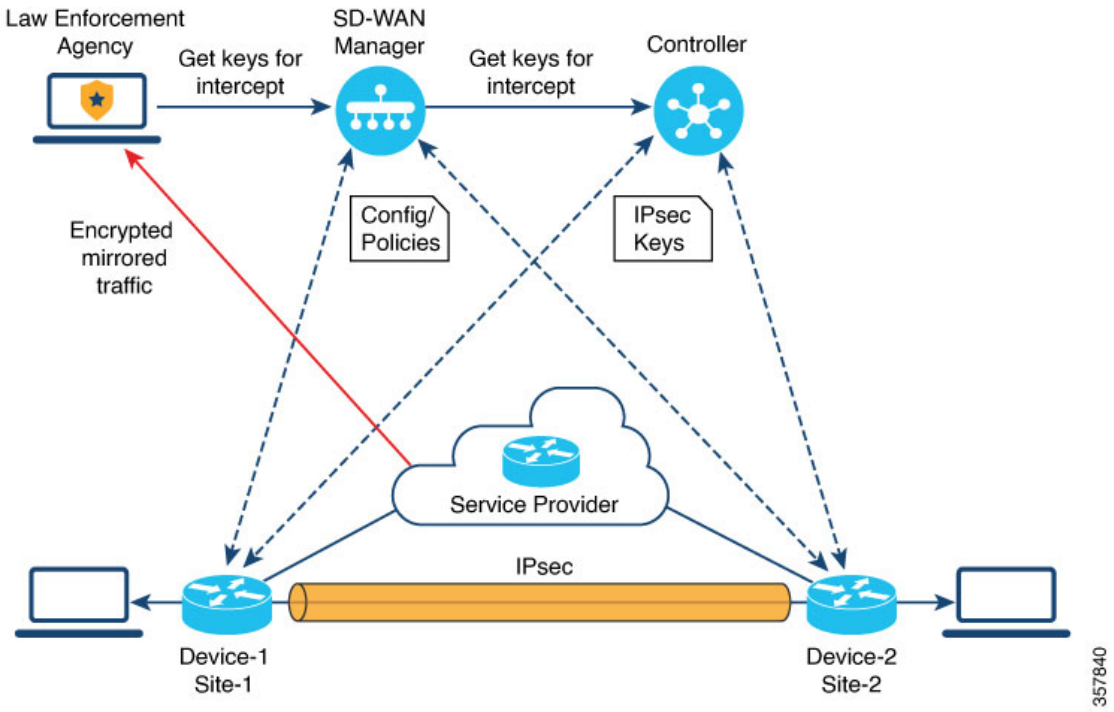
機能名	リリース情報	説明
合法的傍受 2.0 の拡張機能	Cisco vManage リリース 20.10.1	これは、Cisco Catalyst SD-WAN の合法的傍受機能で使用可能な Cisco SD-WAN Manager GUI およびトラブルシューティング オプションを強化する機能です。 • Cisco SD-WAN Manager GUI 拡張機能は次のとおりです。 • Cisco SD-WAN コントローラ で新たに設定された傍受設定を同期するための [vSmart に同期（Sync to vSmart）] ボタン。 • 傍受設定を有効または無効にするトグルボタン。 • 同期とアクティブ化のステータスを表示する進行状況ページ。 • 新しい合法的傍受タスクを示す、Cisco SD-WAN Manager ツールバーのタスクリストアイコンの赤い点。 • アクティブおよび完了した合法的傍受タスクのリストを表示するタスクリストペイン。 • Cisco SD-WAN コントローラ からキー情報または傍受関連情報（IRI）を取得するための傍受取得オプション **Get IRI**。 • デバッグログと管理技術ファイルを使用して、Cisco SD-WAN コントローラ および Cisco SD-WAN Manager をトラブルシューティングする機能。
合法的傍受 2.0 の拡張機能	Cisco Catalyst SD-WAN Manager リリース 20.12.1	これは、合法的傍受をマルチテナントモードに拡張し、Cisco SD-WAN Manager クラスタのサポートを行えるようにする機能です。Cisco SD-WAN Manager クラスタの詳細については、「クラスタの管理」を参照してください。

合法的傍受 2.0 について

Cisco Catalyst SD-WAN の合法的傍受機能により、LEA は分析または証拠のためにネットワークトラフィックのコピーを取得できます。これは、トラフィックミラーリングとも呼ばれます。Cisco Catalyst SD-WAN の『Policies Configuration Guide』の「合法的傍受」の章を参照してください。

Cisco vManage リリース 20.9.1 以降、Cisco Catalyst SD-WAN は次の図に示すように、合法的傍受の新しいアーキテクチャを実装します。

図 *1* : 合法的傍受 *2.0* アーキテクチャ



新しいアーキテクチャには次のような特長があります。

- トラフィックミラーリングは Cisco Catalyst SD-WAN の範囲外です。LEA は、対応するサービスプロバイダーと連携して、ミラーリング用のネットワークトラフィックをキャプチャします。

（注） 上の図では、サービスプロバイダーはアンダーレイ接続で、IPsec トンネルはオーバーレイ接続です。

- キャプチャされたネットワークトラフィックは暗号化されているため、Cisco SD-WAN Manager と Cisco SD-WAN コントローラ は LEA にキー情報を提供します。

- LEA は Cisco SD-WAN Manager からキーを取得して、Cisco Catalyst SD-WAN IPsec トラフィックを復号します。LEA は、各キー再生成期間中にキー情報が取得されるようにします。キー再生成期間は、サービスプロバイダーによって提供されます。キーの取得の詳細については、傍受内容の回収 （8 ページ） を参照してください。キー再生成期間の詳細については、「Configure Data Plane Security Parameters」を参照してください。

合法的傍受管理者は、傍受を設定し、合法的傍受を実行する合法的傍受 API ユーザーを作成する全責任を負います。Cisco SD-WAN Manager 管理者は、合法的傍受管理者のアカウントを作成できます。管理者は、**li-admin** グループのメンバーである必要があります。合法的傍受管理者のアカウント作成の詳細については、「合法的傍受管理者の作成（Create Lawful Intercept Administrator）」を参照してください。

Cisco Catalyst SD-WAN の合法的傍受 2.0 の前提条件

- Cisco SD-WAN コントローラ は **vManage モード**に設定する必要があります。
- Cisco Catalyst SD-WAN での IPsec トラフィックの復号の詳細については、シスコサポートまたはシスコの営業チームにお問い合わせください。

Cisco Catalyst SD-WAN の合法的傍受 2.0 の利点

- 合法的傍受用にエッジデバイスを設定する必要はありません。

（注） 傍受を設定するには、管理者が傍受に含める必要があるエッジデバイスを選択する必要があります。これが必要なのは、Cisco SD-WAN Manager から取得されるキー情報には、選択したデバイスのキーも含まれるためです。

- サービスプロバイダーは、傍受のためにデータトラフィックをキャプチャします。トラフィックはエッジデバイスからは傍受されません。

合法的傍受 2.0 のワークフローの設定

（注） 合法的傍受機能は、Cisco SD-WAN Manager を通してのみ設定でき、CLI では設定できません。

Cisco SD-WAN Manager で合法的傍受を設定するには、次の手順を実行します。

1. 合法的傍受管理者の作成

2. 合法的傍受 API ユーザーの作成
3. 傍受案件の作成

合法的傍受管理者の作成

Cisco SD-WAN Manager の管理者アカウントを使用して、合法的傍受管理者のアカウントを作成します。

1. Cisco SD-WAN Manager メニューから、**[管理（Administration）]** > **[合法的傍受（Lawful Intercept）]** の順に選択します。
2. [ユーザーの追加（Add User）] をクリックして、合法的傍受管理者ユーザーアカウントを作成します。
3. [氏名（Full Name）] フィールドに、合法的傍受管理者の氏名を入力します。
4. [ユーザー名（User Name）] フィールドに、合法的傍受管理者のユーザー名ーを入力します。ユーザー名の先頭には**「li-」**が付きます。
5. [パスワード（Password）] フィールドに、合法的傍受管理者のパスワードを入力します。
6. [パスワードの確認（Confirm password）] フィールドで、パスワードを確認します。
7. [ユーザーグループ（User Group）] ドロップダウンリストから [li-admin] を選択し、[追加（Add）] をクリックします。

   新しく作成された合法的傍受管理者ユーザーアカウントが [ユーザー（Users）] ウィンドウに表示されます。

合法的傍受 API ユーザーの作成

合法的傍受 API ユーザーアカウントは、ログインし、Cisco SD-WAN Manager の REST API を使用してキー情報を取得する LEA のユーザー用です。Cisco Catalyst SD-WAN IPsec トラフィックの合法的傍受を実行するユーザーです。

LEA では
`https://{vmanage_ip}/dataservice/li/intercept/retrieve/<intercept_id>`
を使用して、キー情報を取得します。

合法的傍受 API ユーザーを作成するには、次の手順を実行します。

1. 合法的傍受管理者として Cisco SD-WAN Manager にログインします。

（注） 合法的傍受管理者が Cisco SD-WAN Manager にログインすると、Cisco SD-WAN Manager メニューで使用できるのは[モニター（Monitor）]オプションと[管理（Administration）]オプションのみです。

2. Cisco SD-WAN Manager メニューから、**[管理（Administration）]** > **[合法的傍受（Lawful Intercept）]** の順に選択します。
3. [ユーザーの追加（Add User）] をクリックして、合法的傍受 API ユーザーアカウントを作成します。
4. [氏名（Full Name）] フィールドに、合法的傍受 API ユーザー氏名を入力します。
5. [ユーザー名（User Name）] フィールドに、合法的傍受 API ユーザー名を入力します。ユーザー名の先頭には**「li-」**が付きます。
6. [パスワード（Password）] フィールドに、合法的傍受 API ユーザーのパスワードを入力します。
7. [パスワードの確認（Confirm password）] フィールドで、パスワードを確認します。
8. [ユーザーグループ（User Group）] ドロップダウンリストから [li-api] を選択し、[追加（Add）] をクリックします。

   新しく作成された合法的傍受 API ユーザーアカウントが [ユーザー（Users）] ウィンドウに表示されます。LEA は、合法的傍受 API ユーザーアカウントを使用して Cisco SD-WAN Manager にログインし、キー情報を取得できます。

傍受案件の作成

サポート対象の最小リリース：Cisco vManage リリース 20.9.1 および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.9.1

傍受データを収集するために傍受案件を設定します。傍受案件を設定するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[管理（Administration）]** > **[合法的傍受（Lawful Intercept）]** の順に選択します。
2. [傍受案件（Intercepts）] タブをクリックし、[傍受案件の追加（Add Intercepts）] をクリックします。
3. Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降のリリース：

   Tenant ドロップダウンリストから、テナントを選択します。テナントの追加に関する詳細は、「新しいテナントの追加」を参照してください。
4. [傍受案件 ID（Intercept ID）] フィールドに、番号を入力します。最小 2 桁、最大 25 桁を入力します。

5. [説明（Description）] フィールドに、傍受案件の説明を入力します。
6. [有効化（Enable）] トグルボタンは、デフォルトで有効になっています。ただし、傍受案件は作成後も非アクティブ状態のままです。
7. **[Next]** をクリックします。

   シングルテナントモードでは、[エッジデバイスの追加（Add Edge Devices）] ポップアップウィンドウに Cisco Catalyst SD-WAN ネットワーク内のすべてのエッジデバイスが表示されます。

   Cisco Catalyst SD-WAN Manager リリース 20.12.1 以降のリリース：

   マルチテナントモードでは、[エッジデバイスの追加（Add Edge Devices）] ポップアップウィンドウに、選択したテナントに関連付けられているすべてのシングルテナントエッジ デバイスが表示されます。
8. 傍受案件に追加する 1 つ以上のエッジデバイス名をクリックし、[次へ（Next）] をクリックします。

   ここで、Cisco SD-WAN Manager から、選択したエッジデバイスのキーが提供されます。

（注） 傍受案件に追加したすべてのエッジデバイスに対して傍受令状を指定します。

   傍受のためにエッジデバイスが追加されると、同じネットワークに接続されているすべてのピアデバイスも合法的傍受に使用できます。
9. [LI APIユーザーの追加（Add LI API users）] ページには、合法的傍受管理者によって作成されたすべての LI-API ユーザーが表示されます。
10. 1 つ以上のユーザー名をクリックして傍受案件に追加します。ここで選択したユーザーは、傍受に必要なキー情報を Cisco SD-WAN Manager から取得できます。傍受案件用にキーを取得する方法については、傍受内容の回収を参照してください。
11. [サマリー（Summary）] をクリックします。

    傍受案件の概要が表示されます。
12. [Submit] をクリックします。` [傍受案件（Intercepts）] ページに、設定した傍受案件が表示されます。
13. [vSmart に同期（Sync to vSmart）] をクリックして、Cisco SD-WAN Manager で設定された傍受案件設定を Cisco SD-WAN コントローラ と同期します。

    進行状況ページに、同期とアクティブ化のステータスが表示されます。同期が成功すると、[アクティブ状態（Activate State）] フィールドに緑色のチェックマークが表示されます。

（注） [アクティブ状態（Activate State）] フィールドには、Cisco SD-WAN コントローラ が **vManage** モードに設定されている場合にのみ、緑色のチェックマークのステータスが表示されます。

追加の合法的傍受タスクがある場合は、Cisco SD-WAN Manager ツールバーのタスクリストアイコンに赤い点が表示されます。タスクリストアイコンをクリックすると、アクティブな状態になっている完了したすべての合法的傍受タスクのリストが表示されます。合法的傍受タスクは、最新 500 件まで表示できます。

傍受案件が変更されると、[vSmart に同期（Sync to vSmart）] ボタンが有効になります。[vSmart に同期（Sync to vSmart）] をクリックして、Cisco SD-WAN Manager の傍受案件設定を Cisco SD-WAN コントローラ と同期します。

（注） [vSmart に同期（Sync to vSmart）] ボタンは、新しい傍受案件が作成された場合、または傍受案件が編集または削除された場合にのみ有効になります。

傍受に必要なキー情報を取得するには、[…] をクリックし、[IRIの取得（Get IRI）] をクリックします。IRI は Cisco SD-WAN コントローラ から取得され、Cisco SD-WAN Manager に表示されます。

傍受内容の回収

こうした情報は、MSP によってキャプチャされたトラフィックを復号するために必要であるため、LEA は定期的にキー情報を取得する必要があります。

LEA は、Cisco Catalyst SD-WAN Manager REST API を使用してキー情報を取得できます。

1. LEA は、合法的傍受 API ユーザーとして Cisco SD-WAN Manager にログインします。
2. 合法的傍受 API ユーザーが認証されると、LEA はキー情報を取得する傍受 ID を指定する Cisco SD-WAN Manager REST API を使用して、リクエストを送信します。
3. LEA からのリクエストを Cisco SD-WAN Manager が受信すると、Cisco SD-WAN Manager は、傍受設定がされている Cisco SD-WAN コントローラ に要求を転送します。
4. Cisco SD-WAN コントローラ は次に、指定された傍受案件 ID のキー情報を取得し、キー情報を JSON 形式で Cisco SD-WAN Manager に返します。

Cisco SD-WAN Manager による合法的傍受のための Cisco SD-WAN コントローラ トラブルシューティング

サポート対象の最小リリース：Cisco vManage リリース 20.10.1 および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.10.1

Cisco SD-WAN Manager では、デバッグログと admin-tech ファイルを提供して、Cisco SD-WAN コントローラ および Cisco SD-WAN Manager のいかなる問題もトラブルシューティングできるようにしています。

デバッグ ログ

Cisco SD-WAN Manager の Cisco SD-WAN コントローラ をトラブルシューティングするために、デバッグログを使用します。

Cisco SD-WAN Manager でデバッグログを表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから、**[管理（Administration）]**> [合法的傍受（Lawful Intercept）] の順に選択します。
2. [Devices] タブをクリックします。
3. デバッグログを表示するデバイスの横にある [...] をクリックし、[デバッグログ（Debug Log）] を選択します。
4. [ログファイル（Log Files）] ドロップダウンリストで、ログファイル名を選択します。

   ウィンドウの下部にログ情報が表示されます。

Admin-tech ファイル

Cisco SD-WAN Managerの Cisco SD-WAN Manager および Cisco SD-WAN コントローラ をトラブルシューティングするために、デバッグログと admin-tech ファイルを使用します。Admin-tech ファイルの生成に関する詳細については、「Admin-tech ファイルの生成」を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。