Umbrella ローミング セキュリティ

Umbrella ローミング セキュリティ モジュールには、Professional、Insights、Platform、MSP のいずれかのパッケージでの Umbrella ローミング セキュリティ サービスのサブスクリプションが必要です。Umbrella ローミングセキュリティはアクティブな VPN がないときに DNS レイヤセキュリティを提供し、Cisco Umbrella サブスクリプションはインテリジェントプロキシを追加します。さらに、Cisco Umbrella サブスクリプションはコンテンツ フィルタリング、複数ポリシー、強力なレポート、Active Directory の統合などの機能を提供します。サブスクリプションに関係なく、同じ Umbrella ローミング セキュリティ モジュールが使用されます。

Umbrella ローミング セキュリティ モジュールのプロファイル（OrgInfo.json）は、各展開を対応するサービスに関連付け、対応する保護機能は自動的に有効化されます。

Umbrella ダッシュボードは、Umbrella ローミング セキュリティ モジュールから発信されるすべてのインターネットアクティビティについてリアルタイムの可視性を提供します。ポリシーおよびレポートの精度のレベルは Umbrella サブスクリプションによって異なります。

サービス レベル サブスクリプションごとに含まれる機能の詳細な比較については、https://umbrella.cisco.com/products/packages を参照してください。

- Android 用の Cisco Secure Client Umbrella モジュール （1 ページ）
- Android Windows または OS 用の Cisco Secure Client Umbrella モジュール （3 ページ）

Android 用の Cisco Secure Client Umbrella モジュール

Android OS の Cisco Secure Client のための包括モジュールは、DNS レイヤ保護を提供する管理対象 Android デバイスのローミングクライアントです。この保護は、Android ワークプロファイルでカバーされるアプリケーションとブラウジングの両方に拡張されます。

モバイルデバイス管理システム (MDM) は、このクライアントを Android デバイスに展開し、Umbrella 設定を Android デバイスにプッシュするために必要です。サポートされている MDM およびその他の前提条件のリストについては、「Android OS で Cisco Secure Client の Umbrella モジュールを展開するための前提条件」を参照してください。

一部の Cisco Secure Client 機能では、Android での Umbrella 機能に制限がある場合があります。

- アプリケーションごとの VPN は、OS の制限により、Umbrella モジュールでは機能しません。リモートアクセス VPN がアクティブな場合、Umbrella による保護は、トンネルされ

た VPN によってトンネリングされた DNS トラフィックにのみ適用されます。アプリケーションごとの VPN に対してリモートアクセスが設定されている場合は、トンネル化されたアプリケーションの DNS トラフィックに対してのみ、Umbrella による保護が適用されます。

- ロックダウン（フェールクローズ）オプションを使用して、常時接続 VPN を使用しないでください。VPN サーバに到達できない場合、インターネットアクセスを停止します。常時接続 VPN がオンに設定されている場合にロックダウン設定をオフにするには、MDM ガイドを参照してください。

Umbrella 完全機能セットの説明については、「Umbrella Module for AnyConnect (Android OS)」を参照してください。

Android OS で Cisco Secure Client の Umbrella モジュールを展開するための前提条件

（注） Cisco Secure Client は、MDM で作成されたワークプロファイル内のアプリとブラウザから生成されたトラフィックをモニタし、それに応じて閲覧をブロックまたは許可します。アプリケーションやブラウザによってワークプロファイルの外部で生成されたトラフィックはモニタされません。

- ソフトウェアを展開し、Umbrella 設定をモバイルデバイスにプッシュするためのモバイルデバイス管理システム（MDM）。現在テスト済みのバージョンは、Mobile Iron、Meraki、VMWare Workspace 1（AirWatch）、または Microsoft Intune です。
- Android OS バージョン 6.0.1 以降を搭載した Android（Samsung/Google Pixel）モバイルデバイス。
- DNS ポリシーの設定、登録済み Android デバイスの管理、およびレポートのための Umbrella ライセンス。
- 機能を有効にするための Umbrella 組織 ID。
- 信頼ネットワーク検出（TND）の場合：
  - Umbrella モジュールは、HTTPS が有効な仮想アプライアンス（VA）を検出すると、それ自身を非アクティブにします。ただし、VA が HTTPS をサポートしていない場合は、Umbrella モジュールが動作を続行します。
  - umbrella_va_fqdns 内のすべての VA FQDN を有効にする必要があります。

Android Windows または OS 用の Cisco Secure Client Umbrella モジュール

Cisco Umbrella アカウントの取得

Umbrella ダッシュボード（http://dashboard.umbrella.com/）は、展開に含める Umbrella ローミング セキュリティ モジュールのプロファイル（OrgInfo.json）を取得できるログインページです。このページでは、ローミング クライアントのアクティビティのポリシーとレポートを制御することもできます。

ダッシュボードからの OrgInfo ファイルのダウンロード

OrgInfo.json ファイルは、Umbrella ローミング セキュリティ モジュールにレポートの送信先と適用するポリシーを知らせる、Umbrella ダッシュボードインスタンスについての詳細情報です。

Umbrella ダッシュボード（https://dashboard.umbrella.com）から OrgInfo.json を取得する必要があります。

[ID（Identities）] メニュー ストラクチャで [ローミング コンピュータ（Roaming Computers）] をクリックし、続いて、ページ左上隅の [+] 記号をクリックします。Umbrella ローミング セキュリティ モジュールまでスクロールし、[モジュールプロファイル（Module Profile）] をクリックします。特定のインストール/展開手順と特定のパッケージおよびファイルについては、Cisco Secure Client 展開の概要を参照してください。

（注） OrgInfo.json ファイルを初めて展開すると、データ サブディレクトリ（/umbrella/data）にコピーされて、他のいくつかの登録ファイルも作成されます。したがって、OrgInfo.json 置換ファイルを展開する必要がある場合は、このデータ サブディレクトリを削除する必要があります。または、Umbrella ローミング セキュリティ モジュールをアンインストールし（データ サブディレクトリが削除されます）、新しい OrgInfo.json ファイルを再インストールすることもできます。

Umbrella ローミング セキュリティの起動と実行

Cisco Secure Client を展開するとき、Umbrella ローミング セキュリティ モジュールは、追加機能を有効にするために含めることができるオプションモジュールの 1 つです。

Umbrella ローミング セキュリティ モジュールのステータスおよび状態に関する説明については、『The AnyConnect Plugin: Umbrella Roaming Security Client Administrator Guide』[英語] を参照してください。

OrgInfo.json ファイルの設定

OrgInfo.json ファイルには、Umbrella ローミング セキュリティ モジュールにレポートの送信先と適用するポリシーを知らせる、Umbrella サービスサブスクリプションについての詳細が含まれています。OrgInfo.json ファイルを展開し、CLI または GUI を使用して Cisco Secure Firewall ASA または ISE から Umbrella ローミング セキュリティ モジュールを有効にすることができます。次の手順では、最初に Cisco Secure Firewall ASA から有効にする方法、次に ISE から有効にする方法を示します。

Secure Firewall ASA CLI

1. Umbrella ダッシュボード（https://dashboard.umbrella.com）から Cisco Secure Firewall ASA ファイルシステムに取得した OrgInfo.json をアップロードします。
2. 設定に応じてグループ ポリシー名を適切に調整して、次のコマンドを実行します。

```
webvpn
 anyconnect profiles OrgInfo disk0:/OrgInfo.json

group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

1. **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnectクライアントプロファイル（AnyConnect Client Profile）]** に移動します。
2. [追加（Add）] を選択します。
3. プロファイルの名前を入力します。
4. [プロファイルの使用（Profile Usage）] ドロップダウン メニューから Umbrella セキュリティ ローミング クライアント タイプを選択します。OrgInfo.json ファイルが、[プロファイルの場所（Profile Location）] フィールドに入力されます。
5. [アップロード（Upload）] をクリックして、ダッシュボードからダウンロードした OrgInfo.json ファイルの場所を参照します。
6. [グループ ポリシー（Group Policy）] ドロップダウン メニューで DfltGrpPolicy に関連付けます。グループ ポリシーで新しいモジュール名を指定するには、追加の Cisco Secure Client モジュールの有効化を参照してください。

ISE

ISE からイネーブルにするには、以下の手順に従います。

1. Umbrella ダッシュボード（https://dashboard.umbrella.com）から OrgInfo.json をアップロードします。
2. ファイル OrgInfo.xml の名前を変更します。
3. Cisco Secure Client を展開するための ISE の設定の手順に従います。

セキュリティ ポリシーの設定とレポートの確認

保護を受信し、レポート情報を表示し、ポリシーを設定するには、Cisco Umbrella アカウントが必要です。詳細な説明については、https://docs.umbrella.com/product/umbrella/ または https://support.umbrella.com にアクセスして追加情報を参照してください。

インストール後 90 分から 2 時間以内に、ローミング コンピュータが Umbrella ダッシュボードに表示されます。https://dashboard.umbrella.com に移動して認証し、**[ID（Identities）] > [ローミング コンピュータ（Roaming Computers）]** の順にアクセスすると、ローミング クライアントのリスト（アクティブ クライアントと非アクティブクライアントの両方）とインストールされている各クライアントの詳細が表示されます。

最初は、セキュリティ フィルタリングが基本レベルのデフォルトのポリシーがローミング コンピュータに適用されています。このデフォルトのポリシーは、ダッシュボードの [ポリシー（Policies）] セクション（または [設定（Configuration）] > [Cisco Umbrella アカウントのポリシー（Policy for Cisco Umbrella accounts）]）にあります。

ローミング クライアントのレポートは、[レポート（Reports）]セクションにあります。Umbrella ローミング セキュリティ モジュールがインストールされ VPN がオフにされているコンピュータからの DNS トラフィックを確認するには、アクティビティ検索レポートをチェックします。

診断の解釈

Umbrella ローミング セキュリティ モジュールの問題を診断するには、DART レポートを実行する必要があります。実行方法については、こちらを参照してください。Umbrella の問題とトラブルシューティングの詳細については、Cisco Umbrella Troubleshooting を参照してください。

SWG デバッグロギング

SWGConfigOverride.json ファイルを SWG フォルダにコピーすることで、デバッグロギングを有効にできます。SWGConfig.json に値が存在する場合、SWGConfigOverride.json の設定値は、そのログレベル {"logLevel":"1"} と自動チューニング {"authtuning:"1"} 設定をオーバーライドします。SWG フォルダの場所は次のとおりです。

- Windows（Secure Client）：C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG
- macOS（Secure Client）：/opt/cisco/secureclient/umbrella/swg

オーバーライドファイルをコピーした後、SWG サービス（または Cisco Umbrella サービス）を再起動する必要があります。

SWGConfigOverride.json ファイルを適切な SWG フォルダにコピーしたら、次の手順を実行してデバッグロギングを有効にします。

- macOS の場合：Secure Client エージェントを停止および起動する手順については、https://support.umbrella.com/hc/en-us/articles/230561067#Roaming-Client-for-OS-X5 を参照してください。

- Windows の場合：サービス MMC スナップイン（[開始（Start）] > [実行（Run）] > [Services.msc]）を介して Cisco Secure Web Gateway（4.10.x ビルドでは acswgagent/5.x ビルドでは csc_swgagent）サービスを再起動するか、停止して起動します。

Umbrella ローミング セキュリティ モジュール

Umbrella ローミング セキュリティ モジュールは DNS レイヤのセキュリティを提供しますが、Cisco Secure Client Umbrella セキュア Web ゲートウェイ（SWG）エージェントモジュールはエンドポイントでのセキュリティレベルを提供し、より多くの展開シナリオで柔軟性と潜在能力が高まります。Umbrella セキュア Web ゲートウェイでは、オフプレミスとオンプレミスの両方のシナリオにおいて、Web トラフィックを安全に認証およびリダイレクトすることができます。この実装には、Umbrella からの SIG Essentials または SIG アドオンサブスクリプションが必要です。

セキュア Web ゲートウェイクライアントは、暗号化されたヘッダーを HTTP 要求に挿入し、ヘッドエンドはそのヘッダーを抽出して復号化し、ユーザーデータを使用してアイデンティティおよびポリシーの決定と適用を行います。同様に、HTTPS トラフィックの場合、セキュア Web ゲートウェイクライアントは SWG ヘッドエンドで HTTP 接続要求を開始し、接続要求によって暗号化されたヘッダーが伝送されます。このヘッダーは抽出、復号化され、アイデンティティ/ポリシーの決定と適用に使用されます。

デフォルトでは、セキュア Web ゲートウェイはポート 80 および 443 で HTTP または HTTPS トラフィックを代行受信します。Umbrella クラウド設定では、非標準ポート（80 および 443 以外）を追加できます。これを設定すると、セキュア Web ゲートウェイはデフォルトの標準ポートに加えて、これらの追加ポートで HTTP/HTTPS トラフィックをリッスンします。

信頼ネットワーク検出では、ユーザーは信頼ネットワーク上でセキュア Web ゲートウェイを非アクティブ化することを選択できます。この設定が Umbrella クラウドで設定されている場合に、AnyConnect VPN トンネルの状態がアクティブである場合、信頼ネットワーク上ではセキュア Web ゲートウェイ機能は無効になります。[UI統計（UI Statistics）] ウィンドウに表示される [Web保護ステータス（Web Protection Status）] には、状態の変更が反映されます。

（注） この設定を構成すると、Umbrella の DNS 保護状態によって決定される特定のエラー（Umbrella リゾルバが到達不能な場合など）の場合にもセキュア Web ゲートウェイが非アクティブになります。

プロキシされてはならないドメインまたは IP アドレスは、[展開（Deployments）] > [ドメイン管理（Domain Management）] の下にある全てのダッシュボードで定義できます。ワイルドカードはサポートされていませんが、Umbrella は親ドメインに属するすべてのサブドメインと一致します。 たとえば、example.com がドメイン管理リストに入力された場合、www.example.com も一致し、バイパスされます。Classless Inter-Domain Routing（CIDR）表記法を使用して IP アドレスを入力します。現在、IPv4 アドレスのみがサポートされています。

Cisco Secure Client が Umbrella プロキシへの接続を設立できない場合、Cisco Secure Client はデフォルトで設立することに失敗し、ユーザーがダイレクトアクセスできるようになってしまいます。このハードコードされた動作は設定できません。

これらのすべての Umbrella UI 設定の詳細については、『Cisco Umbrella SIG User Guide』[英語] を参照してください。

セキュア Web ゲートウェイの制限事項

- Cisco Secure Client がインストールされているローカルホストもプロキシ自動設定（PAC）ファイルで設定されているシナリオでは、PAC ファイルが Cisco Secure Client よりも優先されます。
- 現在、IPv4 のみがサポートされています。
- ローカルプロキシはサポートされていません。
- インストール後、Umbrella セキュア Web ゲートウェイエージェントが Umbrella クラウドと同期し、その設定を受信するまでに最大で 50 分かかることがあります。ただし、デフォルトの Web ポリシーは、同期が発生するまで適用されます。

Umbrella SWG のインストールおよびアップグレード

Cisco Secure Client Umbrella のセキュア Web ゲートウェイモジュールは、Windows または macOS でのみ使用できます。Cisco Secure Client の UI で VPN 機能を無効にし、VPN タイルを非表示にするオプションがあります。AnyConnect VPN が Cisco Secure Client Umbrella のセキュア Web ゲートウェイエージェントとともにインストールされている場合は、VPN プロファイルで *AllowLocalProxyConnections* 設定を有効にする必要があります。

Cisco Secure Firewall ASA または ISE 経由の事前展開と Web 展開の両方がサポートされています。

Umbrella SWG のログファイルとメッセージ

Cisco Umbrella は、SWGConfig.json ファイルの形式で Cisco Secure Client SWG モジュールに設定情報を送信します。設定ファイルの SWGConfig.json は次の場所に保存されます。

- Windows—C:\ProgramData (x86)\Cisco\Cisco Secure Client\Umbrella\SWG
- macOS—/opt/cisco/secureclient/umbrella/swg/

Umbrella ローミングセキュリティタイルのステータス

セキュア Web ゲートウェイの状態は [詳細統計（Advanced Statistics）] ウィンドウで確認できます。このウィンドウの Umbrella ローミング セキュリティ タイルでは、Web 保護ステータスが次のいずれかによって示されます。

- 無効（Disabled）：Umbrella サービスがダウンしています
- 保護済み（Protected）：cscswgagent が実行中です。

- 未保護（Unprotected）：cscswgagent が実行されていません。
- 設定エラー（Config Error）：SWGConfig.json の値が正しくありません。
- クラウドサービス利用不可（Cloud Service Unavailable）：Umbrella プロキシに到達できません。

Umbrella セキュア Web ゲートウェイエージェントの詳細統計については、Cisco Secure Client UI を開き、Umbrella ローミング セキュリティ ブランチに移動して、Umbrella プロキシにリダイレクトされた HTTP リクエストの数、Umbrella プロキシにリダイレクトされた HTTPS リクエストの数、プロキシへのリダイレクトに失敗したリクエストの数、および Cisco Secure Client 接続先の Umbrella プロキシを表示することもできます。エラーおよび情報メッセージは、メッセージ履歴に記録されます。

Umbrella セキュア Web ゲートウェイのトラブルシューティング

DART バンドルを実行する際、[ログファイルの選択（Log File Selection）] ウィンドウで Cisco Secure Client Umbrella ローミング セキュア モジュールをオンにしている場合は、SWGConfig.json および SWG 関連のログが追加されます。http://httpbin.org/ip に移動して、トラフィックが Umbrella プロキシに到達しているかどうかを確認します。接続のリセットが発生する場合は、HTTP 要求を送信して応答コードを確認してください。

- HTTP 応答コードが 452 の場合は、クライアントのクロックが同期されているかどうか、またはタイムスタンプに誤りがあるかどうかを確認します。悪意のあるユーザがヘッダーのリプレイを試みている可能性があります。
- HTTP 応答コードが 401 の場合は、キーは最新ではありません。Umbrella ダッシュボードでデバイスの最後の同期時刻を確認します。

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。