

# Cisco Umbrellaユーザのためのベストプラクティス

## 内容

---

[はじめに](#)

[Cisco Umbrellaサービスの健全性とシステムステータス](#)

[ネットワーク登録](#)

[ローカルファイアウォールとプロキシ](#)

[ロールアウトフェーズ](#)

[インテリジェントプロキシ/ブロックページ](#)

[Cisco Umbrella仮想アプライアンス](#)

[サードパーティ製品との統合](#)

[Active Directoryの統合](#)

[クライアントのローミング](#)

[Logging](#)

[マネージドサービスコンソールのベストプラクティス](#)

[2要素認証](#)

[Cisco Umbrellaサポートチームへの連絡と協力](#)

---

## はじめに

このドキュメントでは、Cisco Umbrellaに関連するさまざまなベストプラクティスについて説明します。

## Cisco Umbrellaサービスの健全性とシステムステータス

- ローカルDNSが使用できない場合でもUmbrellaシステムステータスページを確認できるように、<http://208.69.38.170/>と<https://146.112.59.2/#/>をブックマークに登録します。
- サービスの品質低下、サービスの停止、メンテナンスとイベントに関する通知を受け取るには、<https://146.112.59.2/#/>でCisco Umbrellaサービスステータスページに登録します。
- Cisco Umbrellaナレッジベースのサービスアップデートおよびアナウンスページに従ってください。
- Cisco Umbrellaダッシュボードの「メッセージセンター」で、製品アラートと通知を定期的に確認します。

## ネットワーク登録

組織に関連付けられているすべてのIPアドレスとIPアドレスのCIDR範囲は、Umbrellaに登録されている必要があります。詳細については、[Umbrellaのドキュメントを参照してください。](#)

## ローカルファイアウォールとプロキシ

- Umbrella IPアドレスのCIDR範囲を許可するようにローカルファイアウォールを設定します。
- HTTPプロキシを使用する場合は、設定されていることを確認します。

## ロールアウトフェーズ

- 可能な限り、段階的に展開し、大規模に展開する前にテストします。新しい機能をテストするには、ユーザーとコンピューターのサブセットにポリシーを適用します。テストが正常に完了したら、ポリシーを適用するユーザーとコンピューターの数を増やします。
- ポリシーテスターを使用して、IDおよび個々のドメインの目的のポリシー機能を確認します。
- ブラウザでテストページにアクセスして、機能を確認します。詳細については、「How To: Successfully test to ensure you are running Umbrella」を参照してください。
- 1つ以上のスケジュール済みレポートを作成して、セキュリティ関連のイベントに関する環境の監視に役立てます。詳細については、[Umbrella](#)のドキュメントを参照してください。

## インテリジェントプロキシ/ブロックページ

- インテリジェントプロキシ機能を使用する場合、または使用を計画している場合は特に、ロールアウトに[ルートCA](#)を含めます。また、いずれにしろインストールすることをお勧めします。これは、https://の場合にブロックされたサイト(例：<https://facebook.com>)では、インストールされていない場合にエラーが生成されるためです。

## Cisco Umbrella仮想アプライアンス

- 仮想アプライアンス(VA)を使用する場合、導入する前に[内部ドメイン](#)のリストに必要事項を入力してください。
- VMWareで仮想アプライアンスを使用している場合は、VMXNET3アダプタを使用します。
- 仮想アプライアンスを使用している場合は、VMWareまたはHyper-Vホストを介して各VAのコンソールを定期的を確認します。右側には、すべてのServicesエントリとConnectivityエントリが緑色で表示されます。
- 次の説明に従って内部DNSサーバを設定します。Umbrellaを導入する際の内部DNSサーバの推奨設定は何ですか。

## サードパーティ製品との統合

- Check PointやCisco AMP Threat Gridなどの統合を使用している場合は、ブロックしたことがないドメインをGlobal Allow List (またはUmbrellaポリシーに従った他のドメインリスト)に追加します。
  - 組織のホームページ(mydomain.com)。
  - 提供するサービスを表すドメインで、内部レコードと外部レコードの両方を持つことができます(mail.myservicedomain.com、portal.myotherservicedomain.com)。

- Cisco Umbrellaが認識している、または自動ドメイン検証に含まれていない、あまり知られていないクラウドアプリケーションに依存している可能性があります (localcloudservice.com)。

## Active Directoryの統合

- Cisco UmbrellaがActive Directoryと統合されている場合は、[ADユーザ例外リスト](#)にサービスアカウントを追加します。

## クライアントのローミング

- Roaming Clientを使用している場合は、[Internal Domainsリスト](#)に入力されていることを確認します。
- Cisco UmbrellaダッシュボードのIdentities > Roaming Computersで、すべてのRoaming Clientが同じバージョンであることを確認します。
- Cisco Secure Client (以前のAnyConnect) を使用している場合は、スタンドアロンのローミングクライアントではなく、Umbrella Roamingセキュリティモジュールを使用します。
- 航空会社のWi-Fiでローミングクライアントを使用する場合は、「ローミングクライアント」および「航空会社/ホテルのWi-Fiのベストプラクティス」を参照してください。

## Logging

詳細なログは30日間だけ保持され、集約されたレポートデータに分割されます。より詳細なデータのコピーを30日以上保持する場合は、Settings > Log Managementで、データをにエクスポートするAmazon S3バケットを設定します。

## マネージドサービスコンソールのベストプラクティス

Managed Services Console MSP Professional Services Automation(PSA)との統合：

- [PSAと統合されているMSP](#)の場合は、「PSA統合」アイコンが緑色で表示されることを確認します。

## 2要素認証

- Cisco Umbrellaユーザ向けの[2要素認証](#)を**実装する**。
- Cisco Umbrella MSP管理者のための2ステップ認証を実装します。

## Cisco Umbrellaサポートチームへの連絡と協力

- Umbrellaダッシュボードにログインしたら、リクエストページのWebフォームを使用してUmbrellaサポートチームにリクエストを送信します。
- Cisco Umbrellaから電話サポートを購入している場合は、Cisco Umbrellaダッシュボードの右上隅に電話アイコンが表示されます。電話アイコンをクリックすると、サポートの電話番

号が表示されます。

- 問題や質問の詳細を入力します。
- サポートケースには、Umbrella診断ツールの出力を使用してください。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。