官公庁向け Cisco SD-WAN とは

官公庁向け Cisco SD-WAN の概要

セキュリティは、今日のネットワーキング インフラストラクチャの非常に重要な要素です。ネットワーク管理者とセキュリティ担当者は、攻撃や侵害からネットワークを防御することを強く求められています。ハイブリッドクラウドとリモート従業員接続の結果として、ネットワークのセキュリティ境界がなくなりつつあります。

FedRAMP（Federal Risk and Authorization Management Program）は、クラウド サービス プロバイダーを評価、許可、およびモニタリングするための標準的なアプローチを確立する米国政府のプログラムです。

官公庁向け Cisco SD-WAN の中核には暗号化とセキュリティが組み込まれています。

- AWS GovCloud（米国）内に「連邦政府境界」と呼ばれる制限されたスペースを作成します。
- アクセスを、連邦政府の認可を受けたユーザーに制限します。
- すべてのコントローラに対して連邦情報処理標準（FIPS）モードで動作します。
- すべてのデータ接続と制御接続がセキュア ハッシュ アルゴリズム 2（SHA-2）に準拠していることを確認します。
- 拡張ユーザーセッション管理を提供します。
- コントローラレベルでリアルタイム監査を実行します。

- 自動化されたアクション計画とマイルストーン（POA&M）レポートを提供します。
- 特別に許可されていないかぎりすべての HTTP 要求を自動的に拒否する専用の Amazon Virtual Private Cloud（Amazon VPC）をお客様が持つことを可能にします。
- AWS Application Load Balancer（ALB）、AWS Web Application Firewall（WAF）、AWS Shield などの AWS サービスによる保護を保証します。すべての Web サービスは、ALB と WAF の背後にあることで保護されます。また、AWS Shield によって、分散型サービス妨害（DDoS）攻撃から保護されます。
- 環境を維持およびモニタリングするシスコのチームである Cisco Federal Operations のために、ローカルユーザーを使用しないロールベースのアクセスを使用します。

官公庁向け Cisco SD-WAN では、毎月、第三者評価機関（3PAO）によるペネトレーションテストを実施します。これに加えて、Qualys が、毎日、ペネトレーションスキャンを実行します。Qualys は、管理 Amazon VPC のコンポーネントです。詳細は、官公庁向け Cisco SD-WAN のコンポーネント （3 ページ）のセクションを参照してください。

Cisco SD-WAN の一般的なセキュリティ設定の詳細については、『Security Configuration Guide, Cisco IOS XE Release 17.x』を参照してください。

サポートされるプラットフォーム

官公庁向け Cisco SD-WAN でサポートされているプラットフォームの完全なリストについては、Cisco IOS XE SD-WAN デバイス のリリースノートにある「Supported Devices」のセクションを参照してください。

FedRAMP に準拠するには、次のソフトウェアバージョンを実行する必要があります。

デバイス	リリース
Cisco vManage	Cisco vManage リリース 20.3.1
Cisco IOS XE SD-WAN デバイスについて	Cisco IOS XE リリース 17.3.1a

（注） ハードウェアルータを使用している場合は、そのデバイスが TAA に準拠している必要があります。デバイスを注文する場合は、デバイスの SKU に ++ が付加されていることを確認してください。これは、デバイスが TAA に準拠していることを示しています。詳細については、シスコのセールス担当者までお問い合わせください。

対象読者

官公庁向け Cisco SD-WAN のユーザーには、 次の 2 つのタイプがあります。

- お客様（サービスプロバイダー、パートナー、その他のエンドユーザーなど）。
- Cisco Federal Operations（FedOps）：官公庁向け Cisco SD-WAN を維持およびモニタリングするシスコのチーム。

（注） Cisco FedOps はお客様の Amazon VPC にアクセスできません。

官公庁向け Cisco SD-WAN のコンポーネント

官公庁向け Cisco SD-WAN のクラウド境界には、カスタマー Amazon VPC と管理 Amazon VPC が含まれます。お客様ごとに専用のカスタマー Amazon VPC があります。

VPC	コンポーネント	ユーザ アクセス
カスタマー	Cisco SD-WAN ソリューションには、Cisco vManage、Cisco vBond オーケストレーション、Cisco vSmart コントローラ、Cisco IOS XE SD-WAN デバイス、およびその他のアプリケーションが含まれます。	カスタマー

VPC	コンポーネント	ユーザ アクセス
管理	Cisco SD-WAN セルフサービスポータル（SSP）：Cisco SD-WAN オーバーレイネットワークをセットアップおよびモニタリングします。 Cisco vMonitor：システムの脆弱性とシステム障害をモニタリングします。 Cisco vOrchestrator：カスタマー VPC の作成を支援します。 Wazuh サーバー：Wazuh（FIM サーバークライアント）からのデータをモニタリングします。 Qualys：ペネトレーションテストをスキャンします。 Cisco Data Management Service（DMS）：Cisco vManage がお客様のテレメトリデータを送信するためのデータ ストレージ ロケーション サービスを提供します。 Cisco Data Collection Agent（DCA）：システムの正常性に関するデータを収集します。データを Data Collection Service（DCS）にプッシュします。 Cisco Data Collection Service（DCS）：システム内ですべてのテレメトリデータのエントリポイントとして機能します。 Jira（Atlassian）：システムで検出された脆弱性に関するインシデントを自動的に作成する、Jira の強化されたインスタンスを指します。 Amazon Web Services（AWS）Bastionホスト：Cisco FedOps にセキュアなログインメカニズムを提供します。	Cisco FedOps 注：オーバーレイネットワークを管理するために、お客様は、管理 VPC でホストされる Cisco SD-WAN SSP にアクセスできます。

表に示されているコンポーネントに加えて、データのフローを支援するために、官公庁向け Cisco SD-WAN ソリューションでは、Amazon Web Services（AWS）の Simple Queue Service（SQS）、AWS Application Load Balancer（ALB）、AWS Web Application Firewall（WAF）、および Amazon Aurora MySQL データベースが使用されます。管理 Amazon VPC のネットワーク

アクセス コントロール リスト（ACL）は、官公庁向け Cisco SD-WAN が承認した Okta のインスタンスを使用して管理されます。

連邦政府境界

官公庁向け Cisco SD-WAN の連邦政府境界には、カスタマー Amazon VPC と管理 Amazon VPC が含まれます。お客様ごとに独自の Amazon VPC があります。

官公庁向け Cisco SD-WAN の連邦政府境界は、お客様ごとにエントリポイントが 2 つのみの制限的な環境です。

- カスタマー Amazon VPC
- 管理 Amazon VPC

Amazon Virtual Private Cloud へのお客様のアクセス

お客様だけが、そのお客様のカスタマー Amazon VPC にアクセスできます。

お客様がオーバーレイネットワークをセットアップすると、そこには次の Cisco SD-WAN コンポーネントが含まれます。

- Cisco vManage
- Cisco vSmart コントローラ
- Cisco vBond オーケストレーション

お客様がカスタマー Amazon VPC にアクセスする方法

カスタマー Amazon VPC にアクセスするには、信頼できる IP アドレスによるオーバーレイネットワークへのアクセスを可能にすることを、お客様が Cisco SD-WAN SSP に許可する必要があります。

Amazon Virtual Private Cloud への管理アクセス

管理 Amazon VPC は、官公庁向け Cisco SD-WAN ソリューションのセキュアなモニタリングとエンドツーエンドの監査を実現します。Amazon VPC は、許可された IP アドレスとポート番号のセットを持つ Amazon クラウド内のセキュアな場所です。

お客様が管理 Amazon VPC でアクセスできるコンポーネントは、Cisco SD-WAN SSP のみです。Cisco SD-WAN SSP の他のコンポーネントには、Cisco FedOps のみがアクセスできます。

Cisco FedOps が管理 Amazon VPC にアクセスする方法

1. Cisco AnyConnect セキュア モビリティ クライアントを使用してシスコ ネットワークに接続します。
2. Cisco SD-WAN SSPにログインします。

Cisco FedOps ユーザーがログインすると、リクエストが、管理 Amazon VPC へのセキュアシェル（SSH）アクセスを提供する AWS の要塞ホストを通過します。

3. 多要素認証（MFA）には Okta アドバンストサーバーを使用します。

（注） Okta ID プロバイダー（IdP）で指定されたグループに属している許可されたユーザーのみが、AWS の要塞ホストにアクセスできます。

4. ログインが認証されると、Cisco FedOps は、管理 Amazon VPC 内の任意のデバイスに接続できます。

データ フロー

官公庁向け Cisco SD-WAN ソリューションでは、Cisco vMonitor がさまざまなシステムからデータとログを収集して、システムの正常性をチェックし、問題を特定します。Cisco vMonitor は次のソースを使用します。

- Cisco Data Collection Agent（DCA）：これらのエージェントは、官公庁向け Cisco SD-WAN から正常性データを収集するために使用されます。すべての Cisco DCA からのデータは、その後、Cisco Data Collection Service（DCS）に送信されます。
- Wazuh サーバー：Wazuh FIM（File Integrity Monitoring）サーバークライアントからのデータをモニタリングします。官公庁向け Cisco SD-WAN ソリューションのコントローラには、監査ログおよび Syslog の変更を収集する FIM サーバーが組み込まれています。これらの変更は、脆弱性ベクトルを検出するために Wazuh サーバーによってモニタリングされます。Cisco vMonitor サーバーによって収集されたすべてのデータと、脆弱性が、タグ付けされ、POA&M レポートとして提供されます。
- Okta：Cisco vMonitor は、認証およびアクセス試行に関する Okta のログのために、MFA に使用される外部 Okta サーバーをポーリングします。
- Qualys：Qualys は、脆弱性スキャンとコンプライアンススキャンを実行します。このスキャンは、カスタマー Amazon VPC 内にあるすべてのデータと、管理 Amazon VPC 内にあるすべてのコンポーネントに対して毎日実行されます。スキャンの結果は、Cisco vMonitor データベースに記録されます。

すべての接続、データの保存場所、およびファイルインシデント管理イベントが、Cisco vMonitor データベースにプッシュされます。重大な問題が検出されると、Cisco vMonitor データベースは、JIRA チケットと POA & M アラートを生成します。JIRA チケットと POA&M アラートの詳細については、アクション計画とマイルストーンを参照してください。

データは、セキュアな状態を確保するために、AWS S3 バケットに保存されます。すべてのデータ（保管中および転送中）と制御接続は SHA-2 に準拠しています。次のタイプのデータが保存されます。

- 個人識別情報（PII）

- アクセスされたドメイン
- プライベート IP アドレス
- ソリューションにアクセスしたお客様
- ネットワークで発生するスニフィング

Data Collection Agent の設定とモニタリング

Cisco DCA は Cisco vManage の内部で動作するエージェントであり、オンプレミスまたはクラウドでホストできます。この Cisco DCA エージェントは、適切な設定が有効になっているかぎり、統計情報のレポート、モニタリング、および Cisco SD-WAN へのテレメトリデータの提供に使用されます。

これを実現するために、Cisco DCA は、Cisco DMS と呼ばれるサービスとやり取りします。Cisco DMS は、お客様のオーバーレイネットワークに関連する情報（ネットワークが存在する地域、データストレージの設定など）を保持します。Cisco DCA は、お客様のオーバーレイネットワークごとに生成される（および帯域外でお客様に伝達される）カスタム oAuth ログイン情報を使用して、Cisco DMS で自身を認証します。Cisco DMS が Cisco DCA を認証できる場合、前者は後者に認証トークンを与え、Cisco DCA を適切な Cisco DCS にリダイレクトします。

Cisco DCS は、すべてのテレメトリデータを Cisco SD-WAN に取得するためのエントリポイントです。パブリッククラウド、地域などに応じて、Cisco DCS サービスのインスタンスが多数存在する場合があります。Cisco DCA は、前のフローで取得したトークンを使用して Cisco DCS で自身を認証し、地域の Cisco DCS トークンと交換します。その後、このトークンは、すべての種類のデータを Cisco DCS にプッシュするときに Cisco DCA によって使用されます。

Cisco DCA は、Cisco SD-WAN ローカルホストから定期的にデータを収集し、そのデータを Cisco DCS にプッシュします。Cisco DCS は、そのデータを JSON ファイルとして S3 バケットに保存します。S3 バケットが受信する新しい JSON ファイルごとに、new-object-created イベントが AWS Simple Notification Service（SNS）トピックに送信されます。Cisco vMonitor はすでに HTTPS エンドポイントでトピックをサブスクライブしているため、Cisco vMonitor サーバーは、すべての S3 new-object-created イベントについて AWS SNS から HTTPS リクエストを受信します。Cisco vMonitor サーバーは、HTTPS リクエストを検証し、内部のメタデータを使用して S3 上の実際のファイルを取得し、データベースを更新します。

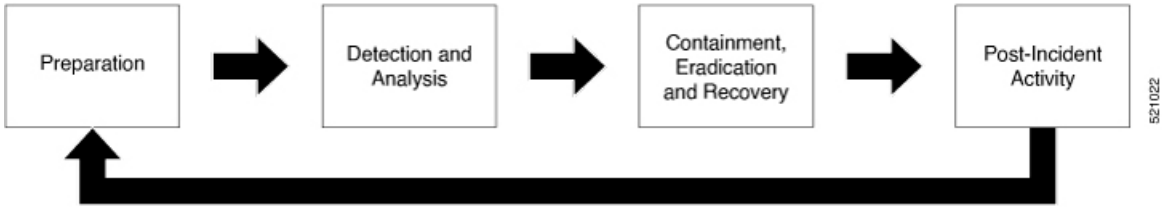
インシデント対応

インシデント対応は、システムのセキュリティインシデントに対応し、レポートする一貫性のある効果的な手段を提供します。これには、通常の情報技術（IT）サービスを迅速に復旧させ、業務への悪影響を最小限に抑えるために実行されるすべてのアクションが含まれます。Cisco SD-WAN は、米国国立標準技術研究所（NIST）Special Publication（SP）800-61、Rev 2 のインシデントの定義にしたがって、インシデント対応チームをアクティブ化するタイミング

を決定します。インシデント対応計画では、シスコのリソースと継続的に連携して、申し出に対してインシデント（存在する場合）を特定し、封じ込め、根絶し、復旧するための備えを維持します。

セキュリティインシデントへの対応は、単一のアクションではなく、全体的なアプローチです。このアプローチにより、問題が確実に検出され、軽減されます。また、このアプローチには、検出された問題（存在する場合）から復旧する手順もあります。これには、次のフェーズが含まれます。

図 *1*: インシデント対応フェーズ



官公庁向け Cisco SD-WAN の使用のワークフロー

官公庁向け Cisco SD-WAN を使用するには、次の手順を実行する必要があります。

1. Cisco SD-WAN セルフサービスポータル にログインします。
2. オーバーレイネットワークを作成します。
3. Cisco vManage を設定します。
4. 追加のセキュリティ機能をセットアップします。
5. 環境をモニタリングおよび管理します。