The bridge to possible

Cisco Advanced Wireless Intrusion Prevention System および不正管理

目次

ソリューションの概要

ワイヤレスは、もはやあると便利なセカンダリネットワークではありません。Wi-Fi 規格の進歩と批准により、同時接続デバイスと Internet of Things（IoT）接続が密集する環境においても、業界を超えて広く使用されるようになりました。現在、ワイヤレスで接続されているデバイスの数は 150 億を超えています。この数は、2021 年末までに 200 億を超えると予想されています（出典：https://www.statista.com/statistics/802706/world-wlan-connected-device/）。従業員とゲストに Wi-Fi アクセスを提供する企業、ホットスポットを提供する公共施設、ワイヤレスで接続する産業用 IoT デバイスなど、さまざまな状況が多くの機会を提供すると同時に、ネットワークに新たな脅威をもたらしています。世界の分散型サービス妨害（DDoS）攻撃の総数は、2018 年の 790 万件から 2023 年には 1,540 万件に倍増すると予測されています（出典：Cisco Annual Internet Report (2018-2023)）。精通したモバイルユーザーは、スマートフォンを使用するだけでワイヤレスネットワークをセットアップできます。これは、ユーザーに接続を提供する一方で、攻撃者の侵入経路となる可能性も秘めています。ハッカーは絶えず変化する脅威で脆弱なワイヤレスネットワークを標的にし続けるため、IT 組織は、組織全体でワイヤレスの脅威を追跡して特定し、コンプライアンスを実証するという課題を常に抱えています。

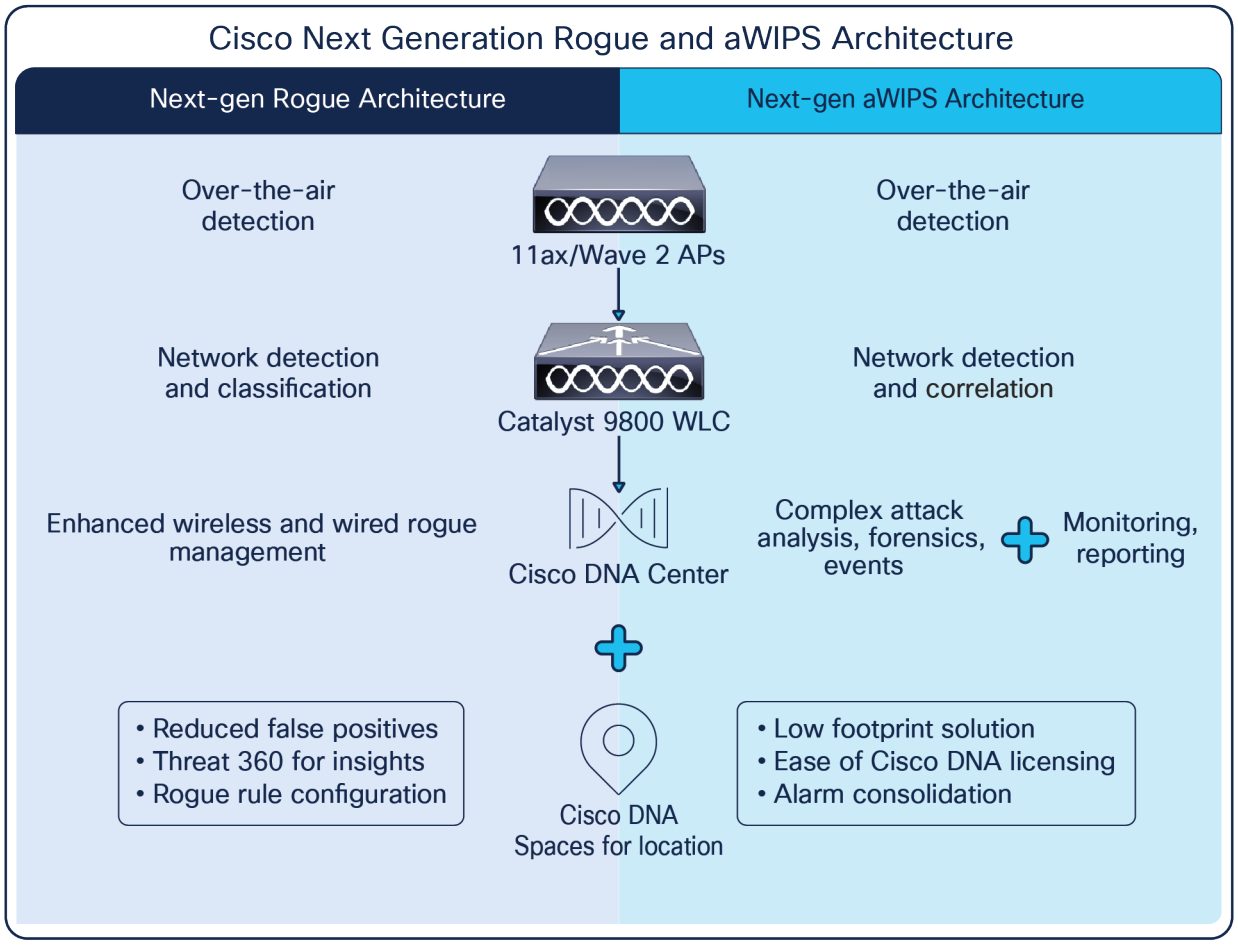

図 1.
Cisco Advanced WIPS および不正管理：システム概要

Cisco Advanced Wireless Intrusion Prevention System（aWIPS）および不正管理は、Cisco DNA Center および Cisco Catalyst インフラストラクチャを使用して有線およびワイヤレスによるレイヤ 1 ~ 3 の不正や脅威を検出し、場所を特定して緩和および封じ込めを行う完結型のワイヤレス セキュリティ ソリューションです。aWIPS を WLAN インフラストラクチャに統合することで、aWIPS サービスと WLAN サービスの両方に同じインフラストラクチャが使用できるようになり、コストを削減し、運用効率を高めることができます。このソリューションは、以下のコンポーネントから構成されています。

- **アクセスポイント：**Cisco CleanAir を搭載したシスコのアクセスポイントは、ビデオカメラや RF 妨害装置などの 802.11 以外の送信元からの攻撃をレイヤ 1 の脅威検出で検出できるように、シリコンベースのインテリジェンスを備えています。アクセスポイントは、無線トラフィックを処理して膨大な数の攻撃や異常にインテリジェントに対応し、ネットワークへの攻撃の有無を判断します。一連の対象プロセスは、拡張性を高められるようエッジで処理されます。アクセスポイントは、Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルを使用して、攻撃対象と攻撃者の MAC アドレス、受信信号強度表示（RSSI）、攻撃時間などの情報を WLAN コントローラにリレーします。Cisco Catalyst 9120 および 9130 アクセスポイントの RF ASIC は、2.4 GHz バンドと 5 GHz バンドのデータ処理無線に影響を及ぼすことなく、すべてのチャネルをスキャンします。
- **Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ：**Catalyst 9800 シリーズには、攻撃の種類を判別するために、不正検出と複数の aWIPS シグニチャのロジックが組み込まれています。Catalyst 9800 シリーズは、不正アクセスポイントなどのセキュリティイベントや進行中の攻撃を検出すると、Cisco DNA Center にアラートを送信し、不正ポリシーの定義に従って不正の脅威を緩和します。
- **Cisco DNA Center：**Cisco DNA Center は、ネットワークの管理、シスコへの投資の最適化、IT 支出の削減などを実現する強力なネットワークコントローラであり、管理ダッシュボードでもあります。

  Cisco DNA Center の不正管理アプリケーションは、脅威を検出して分類し、ネットワーク管理者、ネットワークオペレータ、およびセキュリティオペレータがネットワークの脅威をモニターできるようにします。Cisco DNA Center は、最も優先度の高い脅威を迅速に特定するのに役立ち、Cisco DNA Assurance 内の [Rogue and aWIPS] ダッシュボードでこれらの脅威をモニターできます。このダッシュボードの [Threat 360] ビューには、特定の脅威に関する詳細が表示されます。このビューには、クイックロケーションのマップビューと、影響を受けるすべてのクライアントが含まれます。

Cisco aWIPS および不正管理は、ワイヤレスの脅威を検出して緩和する強力な機能をワイヤレス ネットワーク インフラストラクチャに組み込むことで、業界で最も包括的で正確な、運用効率の高いワイヤレス セキュリティ ソリューションを実現します。

ソリューションのメリット

Cisco aWIPS および不正管理ソリューションは、スタンドアロンのオーバーレイ型 aWIPS および不正管理システムではアーキテクチャ上不可能な機能の上位セットを提供します。Cisco aWIPS および不正管理のインフラストラクチャ統合型アーキテクチャにより、ネットワーク管理者は以下が可能になります。

- **全体を俯瞰する：**一般的な aWIPS ソリューションでは、検出に RF エアモニタリングのみを使用します。Cisco aWIPS および不正管理では、RF エアモニタリングを基盤に、アクセスポイントや WLAN コントローラにネットワークトラフィックや異常を分析する機能を組み込み、デバイスインベントリ分析やネットワーク構成分析のリアルタイム実行で脅威の検出やパフォーマンスの監視を行います。このアプローチにより、より正確、かつ徹底的な検出が可能になります。
- **是正措置を取る：**Cisco aWIPS および不正管理は脅威、脆弱性、パフォーマンスの問題を単に検出するだけでなく、是正措置を可能にします。aWIPS および不正管理は WLAN インフラストラクチャに統合されているため、受動的なモニタリングにとどまらず、インフラストラクチャに介入し、封じ込めを使用してセキュリティの脅威やパフォーマンスの不具合をリアルタイムで修正します。
- **WLAN のフットプリント全体を利用する：**Cisco aWIPS および不正管理は、ネットワーク上のすべてのアクセスポイントを使用して不正なデバイスの場所を特定し、脅威を緩和できます。これにより、場所の精度が高まり、緩和の範囲が広がります。
- **柔軟な展開アーキテクチャによるメリット：**Cisco aWIPS および不正管理では、フルタイムでエアモニタリングを行う専用アクセスポイント、WLAN ユーザーにサービスを提供しているアクセスポイント、またはその両方を使用できます。展開の柔軟性は、ローカル、FlexConnect 中央スイッチング、FlexConnect ローカルスイッチング、SDA などの複数のモードをサポートすることによって提供されます。Cisco DNA Center では、必要に応じてエリア、ビルディング、およびフロアの階層をレイアウトしてネットワークの場所を正確に表すことで、ロケーションに基づいてデバイスをグループ化できます。サイト階層を使用すると、デバイスのグループごとに一意のネットワーク設定と IP スペースを有効にできます。このように柔軟に展開できるため、サイトごとに適正な規模のセキュリティモデルを構築できます。

包括的な保護、正確な検出

エアモニタリング、ネットワークトラフィックと異常の分析、リアルタイムのネットワークデバイスとトポロジの情報、ネットワーク構成の分析を組み合わせたシスコの高度な検出アプローチにより、Cisco DNA Center の Cisco aWIPS 分析、相関、および分類エンジンにイベントの包括的なビューが提供されます。aWIPS は、無線シグニチャだけでは追跡できないイベントを検出し、より正確な検出判定を行うことで、誤検出を減らして有効性を高めることができます。

Cisco aWIPS は、コアの検出機能を基盤として豊富な攻撃の分類を提供し、セキュリティイベントを自動的に分類および緩和するための柔軟なルールをユーザーに提供します。自動分類は、システム本来の正確性により、システムによって検出された潜在的な脅威の手動での調査に関連する運用コストを大幅に削減します。

シスコでは、これらの高度な検出および分類技術と、広範な攻撃、脆弱性、およびパフォーマンス検出ライブラリを組み合わせています。検出されるイベントクラスの例には、不正アクセスポイント/クライアント、ハニーポットや悪魔の双子などのハッカーのアクセスポイント、ネットワーク偵察、アドレスやアイデンティティのスプーフィングなどの AP 偽装、プロトコル攻撃、Denial-of-Service（DoS）攻撃、無線およびネットワークセキュリティの脆弱性、同一チャネル干渉やカバレッジホールなどのパフォーマンスの問題があります。

予防的な侵入防御による aWIPS の補完

ネットワークを保護するための最善の方法は、被害を受ける前に攻撃を阻止するシステムを設計することです。Cisco Catalyst アクセス インフラストラクチャに組み込まれているネットワークセキュリティ強化機能は、Cisco aWIPS ソリューションを補完し、次のような予防的な侵入防御手法を提供します。

- **ネットワークからのセキュリティ攻撃者の排除：**クライアント除外ポリシーにより、高レベルのユーザー認証の失敗や IP アドレスのスプーフィングに自動で対応できます。
- **ネットワーク偵察およびスプーフィング攻撃の防止：**IEEE 802.11w のベースであるシスコ管理フレーム保護により、WLAN 管理フレームを暗号化して認証することで多くの一般的な無線攻撃が防止されます。
- **データの盗難からの保護**：強力なユーザー認証と Wi-Fi Protected Access 3（WPA3）および 802.11i 暗号化規格により、ネットワークへのアクセスと WLAN を通過するデータへのアクセスが保護されます。
- **不正アクセスポイントのロックアウト：**シスコのアクセスポイントで 802.1X 有線ポート認証の LSC プロビジョニングまたは許可リストを使用することで、不正アクセスポイントが有線ネットワークに参加する可能性が実質的になくなります。

機能と利点：技術概要

以降のセクションでは、Cisco aWIPS および不正管理ソリューションの各機能領域と関連する利点について説明します。

不正の検出、分類、および緩和

Cisco aWIPS および不正管理の不正の検出と緩和に関連する機能を表 1 に示します。不正なアクセスポイントとクライアントは、ネットワークへのバックドアアクセスを作成し、ワイヤレスクライアントからデータを盗み出す目的で使用される可能性があります。シスコの不正管理ソリューションは、不正アクセスポイント、不正クライアント、クライアントスプーフィング、クライアントのアドホック接続を検出し、カスタマイズ可能なルールに基づいて自動的に分類して、それらの脅威を緩和します。

表 1. 機能と利点：不正の検出、分類、および緩和

機能	利点
検知	
オンチャネルとオフチャネルのスキャン	802.11 関連スペクトルのすべてのチャネルで、不正アクセスポイント、不正クライアント、クライアントスプーフィング、クライアントのアドホック接続を検出します。
シグニチャベースとネットワーク分析ベースの検出	不正、アドホック、スプーフィングの検出の範囲と精度を高め、スタッフが手動で脅威を調査する時間を短縮します。
CleanAir/スペクトルインテリジェンス	Bluetooth、レーダー、マイクロ波など、802.11 以外の周波数における不正デバイスや DoS 攻撃を検出します。

機能	利点
イベントの分類	
カスタマイズ可能な不正イベントの自動分類	ユーザー定義の分類ルールに基づいて不正イベントの脅威レベルを自動的に分類し、スタッフが介入する必要性を軽減します。
不正なスイッチポートのトレース	検出された不正アクセスポイントがカスタマーネットワーク上にあるかどうかを確認し、スタッフが手動で脅威を評価する必要性を軽減します。
不正デバイスの物理的な場所	不正なアクセスポイントとクライアントをフロアマップにプロットし、スタッフが不正の脅威を評価して簡単に排除できるようにします。CMX または Cisco Spaces と統合することで、ロケーションの精度を向上できます。
緩和	
不正なスイッチポートの無効化	不正アクセスポイントが接続されているイーサネットポートをリモートで無効にし、緩和を加速します。
無線の緩和	展開されたシスコのアクセスポイントを使用して不正なアクセスポイント、クライアント、およびアドホック無線接続を緩和し、緩和を加速および拡張します。
自動または手動による緩和	柔軟な緩和アクションにより、お客様のリスク環境と運用モデルに合わせた調整が可能です。

無線攻撃の検出

Cisco aWIPS の無線攻撃の検出に関連する機能を表 2 に示します。無線攻撃は、RF 環境に隣接するハッカーによって開始されます。RF 信号は壁を通過するため、攻撃者はオフィスの前の駐車場から攻撃してくることもあります。攻撃の種類には、ネットワーク偵察、認証および暗号解読、DoS、偽装の試みのほか、新しい攻撃手法や未知の攻撃手法も含まれます。

表 2. 機能と利点：無線攻撃の検出

機能	利点
攻撃検出の範囲	
ネットワーク偵察およびプロファイリングの検出	トラフィックの動作を分析してパターンマッチングを実行することで、アクセスポイントの偽装、ハニーポット アクセス ポイント、AirDrop セッションなどのツールや手法を検出し、ハッカーが攻撃の手段を探していることを早期に警告します。
認証/解読および脆弱性の悪用の検出	トラフィックの動作を分析してパターンマッチングを実行することで、ファジングビーコン、ファジングプローブ要求、ファジングプローブ応答、不正な形式の関連付け要求、不正な形式の認証、無効な MAC OUI などのツールや手法を検出し、データ盗難の可能性や試みに関するアラートを提供します。

機能	利点
悪意または不注意による DoS の検出	トラフィックの動作を分析してパターンマッチングを実行することで、802.11 プロトコルの不正使用、RF 電波妨害、リソースの枯渇の原因となる認証フラッド、アソシエーションフラッド、Extensible Authentication Protocol over LAN（EAPoL）開始フラッド、PS-Poll フラッド、プローブ要求フラッド 、再アソシエーションフラッド、Request-To-Send（RTS）フラッド、Clear-To-Send（CTS）フラッド、ビーコンフラッドなどのツールや手法を検出し、ネットワークサービスの妨害の可能性や試みに関するアラートを提供します。認証解除フラッド、ディスアソシエーション フラッド、ブロードキャスト認証解除フラッド、ブロードキャスト関連付け解除フラッド、EAPoL ログオフフラッド、認証失敗攻撃、プローブ応答フラッド、ブロック ACK フラッドなど、クライアントに対する DoS 攻撃も検出できます。
偽装およびスプーフィングの検出	トラフィックの動作を分析してパターンマッチングを実行し、認証方式を適用することで、MAC/IP スプーフィング、偽装アクセスポイント、悪魔の双子アクセスポイント、RADIUS サーバースプーフィングなどのツールや手法を検出し、データ盗難の可能性や不正なネットワークアクセスに関するアラートを提供します。
ゼロデイ攻撃の検出	トラフィックの動作を分析することで、新たに導入された攻撃方法や未分類の攻撃方法を検出し、潜在的な脅威に関するアラートを提供します。
脅威と脆弱性の継続的な調査と検出の開発	シスコでは、新たな攻撃手法を発見し、悪用される可能性のあるネットワークの脆弱性についてプロアクティブに分析するために、ワイヤレスの脅威と脆弱性を専門とする調査チームを設置し、Cisco aWIPS の検出機能が常に新たな脅威に対抗できるように取り組んでいます。
イベントの分類と調整	
デフォルトの検出プロファイル	お客様のタイプ別にカスタマイズされたデフォルトの検出調整プロファイルにより、システムの起動から数分で効果的な運用を実現し、システムの調整をすぐに開始できます。
ナレッジベース主導の調整	検出の調整は Cisco DNA Center の脅威ナレッジベースに関連付けられており、攻撃の種類と検出方法のわかりやすい説明と調整のガイダンスが提供されるため、経験が浅いセキュリティオペレータでも調整がさらに容易になります。

セキュリティ脆弱性モニタリング

Cisco aWIPS のセキュリティ脆弱性のモニタリングに関連する機能を表 3 に示します。ワイヤレスネットワークのセキュリティ態勢をリアルタイムで理解することは、攻撃を阻止する上で何よりも重要です。Cisco DNA Center は、ワイヤレスネットワークに脆弱なセキュリティやポリシー違反の設定がないかどうかをプロアクティブかつ永続的にスキャンすることで、自動化された 24 時間体制のワイヤレス脆弱性モニタリングおよびアセスメントを実行します。

表 3. 機能と利点：セキュリティ脆弱性モニタリング

機能	利点
24 時間 365 日の自動設定分析	すべてのワイヤレスコントローラ、アクセスポイント、および管理インターフェイスのセキュリティ設定を分析します。Cisco DNA Center は、無線の脆弱性のスニッフィングだけに依存するのではなく、実際の設定を分析することで、管理プロトコルのセキュリティの分析や、ネットワーク上で動作するセキュリティサービスのアウトオブバンド変更の設定コンプライアンスについての分析など、より正確で詳細な脆弱性分析を提供します。
業界のベストプラクティスまたはカスタム定義のセキュリティポリシーへの準拠の分析	Cisco DNA Center には、ワイヤレスセキュリティ脆弱性アセスメントに関する業界のベストプラクティスがあらかじめ組み込まれています。また、設定監査で、設定が組織の特定のセキュリティポリシーに準拠しているかを分析できます。このデュアルアプローチにより、非常に柔軟で幅広い脆弱性分析が可能になります。
セキュリティアドバイザリによる広範な脆弱性の特定	Product Security Incident Response Team（PSIRT：プロダクト セキュリティ インシデント レスポンス チーム）のスキャンにより、不正な管理アクセスやネットワークアクセス、データ盗難、DoS 攻撃、およびプロトコル攻撃を引き起こす可能性がある脆弱性を特定し、ワイヤレスネットワーク上で実行されるセキュリティサービスにアドバイスを提供します。
aWIPS アラームの統合	事前定義のルールに基づいて aWIPS アラームを統合し、実際の攻撃または脅威を判断するための簡潔な情報をユーザーに提供します。
使いやすいワークフロー	ワイヤレス aWIPS および不正のワークフローでは、aWIPS シグニチャと不正ルールを柔軟に微調整できます。シグニチャを選択したり、不正ルールの条件のシグニチャや脅威レベルのしきい値を設定したりできます。
シグニチャごとのフォレンジック	攻撃を受けた際にシグニチャまたは脅威ごとにトラブルシューティングやデバッグを行えるように、パケットキャプチャを自動的に開始および停止する機能があります。
不正アクセスポイントの影響ゾーン	Cisco DNA Center の [Threat 360] ビューで各アラームの詳細を確認できます。攻撃のコンテキスト、脅威レベル、攻撃の場所と日時が表示されます。

パフォーマンスモニタリングおよび自動最適化

Cisco aWIPS のパフォーマンスモニタリングに関連する機能を表 4 に示します。ネットワークパフォーマンスの低下はネットワークやアプリケーションの可用性に影響を与えますが、悪意のある操作が原因の場合と偶発的な操作が原因の場合があります。無線リソース管理（RRM）を使用して、システムは比類のないパフォーマンスとネットワーク自己修復を提供します。ノイズと干渉に関する情報に加え、クライアントの信号強度やその他のデータを使用して、チャネルを動的に割り当て、アクセスポイントの送信電力をリアルタイムで調整することで、同一チャネル干渉を回避し、障害デバイスを迂回し、カバレッジホールを最小化します。

表 4. 機能と利点：パフォーマンスモニタリングおよび自動最適化

機能	利点
ネットワークの正常性とパフォーマンスの継続的なリアルタイムモニタリング	悪意のある無線干渉と偶発的な無線干渉を防ぎます。
RF ドメインの問題の自動修正	管理者の介入なしで RF ベースの DoS などの問題を解決し、最小限の運用オーバーヘッドでネットワークアップタイムを向上させます。
特殊な RF スキルを必要としない包括的な RF 管理	RF 管理の専門知識がシステムに統合されているため、運用スタッフの負担が軽減されます。

管理、モニタリング、およびレポート

Cisco aWIPS の包括的なセキュリティ管理、モニタリング、およびレポートの機能を表 5 に示します。aWIPS の管理機能は Cisco DNA Center に完全に統合されており、統合された単一のツールでワイヤレスネットワークとワイヤレスセキュリティの両方の運用に対応できます。ワイヤレスネットワークとワイヤレスセキュリティの管理の統合により、アクセスポイントやクライアントデバイスのインベントリとセキュリティポリシーの整合性が維持され、イベントの管理とレポートが簡素化されることで、管理の課題が軽減されます。

表 5. 機能と利点：管理、モニタリング、およびレポート

機能	利点
ワイヤレスネットワークとワイヤレスセキュリティの単一の管理プラットフォーム	
リアルタイムのデバイスインベントリ	アクセスポイントとクライアントデバイスのインベントリが常に最新の状態に維持され、エントリの重複やベンダーの違いによる管理の統合の問題がないため、管理オーバーヘッドを削減しながら高い精度の不正検出が可能です。
仮想管理ドメイン	aWIPS により、ワイヤレスセキュリティの管理とモニタリングを他のワイヤレス管理ロールまたは地域と切り離すことができます。
1 回限りではない管理プラットフォーム	aWIPS と一般的なワイヤレス管理がすべて Cisco DNA Center から実行されるため、プラットフォーム別のスタッフのトレーニングやサポートが軽減されます。
Cisco Unified Wireless Network の機能との統合	aWIPS は、一般的なワイヤレスネットワーク設定、ワイヤレス セキュリティ ポリシー定義、およびロケーションサービスの操作を統合したワークフローを提供します。
コマンドの許可と監査証跡	すべての管理コマンドについて、認証、許可、およびアカウンティング（AAA）で許可できます。ログに記録された設定、調査、および緩和のアクションから管理者まで遡って特定できるため、説明責任を果たすことができます。
企業のスケーラビリティに対応した設計	Cisco DNA Center は非常に大規模な環境に対応するように設計されており、112 コアの Cisco DNA Center アプライアンスごとに最大 96,000 の不正アクセスポイントと 13,000 の aWIPS アクセスポイントがサポートされます。
Cisco DNA Center の [Rogue and aWIPS Assurance] ダッシュボード	
単一の概要ビュー	すべてのセキュリティイベントおよび脆弱性の概要が一目で確認できる合理化された形式で単一の画面に表示されます。イベントのクラスや個々のイベントをマウスでクリックするとドリルダウンでき、日常のモニタリングが簡単になります。
Cisco DNA Center の [Health] ダッシュボード	
単一の概要ビュー	すべてのパフォーマンス関連イベントが一目で確認できる合理化された形式で単一の画面に表示されます。イベントのクラスや個々のイベントをマウスでクリックするとドリルダウンでき、日常のモニタリングが簡単になります。
Cisco DNA Center のイベントの管理とレポート	
包括的なイベントフォレンジック	攻撃に関連するすべてのトラフィックをキャプチャし、調査を容易にします。
スタッフへのイベントのエスカレーション	Cisco DNA Center の [Rogue and aWIPS] ダッシュボードで、重大なイベントに関するアラートをスタッフに自動的に送信し、応答時間を短縮します。
管理者ごとのレポート	履歴レポートを個々の管理者の設定や責任範囲に基づいてカスタマイズできるため、イベント分析が合理化されます。

機能	利点
自動レポートのスケジューリング	履歴レポートを特定の時間に自動的に実行するようにスケジュールできるため、ワークフローが合理化されます。
イベントの保存とアーカイブ	セキュリティ攻撃イベントは Cisco DNA Center に 14 日間保存され、そのまま長期間アーカイブすることもできるため、履歴分析が可能です。

ワイヤレス IP ソフトウェア

- Cisco 802.11ac Wave 2 および 802.11ax のアクセスポイントは、いずれもモニターモードの aWIPS モニタリングおよびクライアントサービスモードのオンチャネルとオフチャネルのスキャンに対応しています。Cisco Catalyst 9120AX および 9130AX シリーズのアクセスポイントには、すべてのチャネルの不正および aWIPS 検出を継続的にモニターする RF ASIC ベースの予備無線が内蔵されています。
- Cisco DNA Center の aWIPS および不正管理の拡張については、『Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide』を参照してください。

ライセンスおよび発注情報

Cisco aWIPS は、Cisco DNA Advantage に含まれるライセンス型ソフトウェア機能セットであり、すべてのリリースで使用できます。シスコの不正管理の機能は、Cisco DNA Essentials ライセンスで使用できます。

具体的なライセンス情報については、『Cisco DNA Software Subscriptions for Access Wireless Ordering Guide』を参照してください。

サービスおよびサポート

シスコでは、お客様のビジネスを支援する多様なサービス プログラムをご用意しています。これらのサービスは、スタッフ、プロセス、ツール、パートナーをそれぞれに組み合わせて提供され、お客様から高い評価を受けています。シスコのサービスは、お客様のネットワーク投資を保護してネットワーク運用を最適化するだけでなく、ネットワーク インテリジェンスの強化や事業拡張に向けた新しいアプリケーションの導入準備という面でもサポートします。シスコサービスの詳細については、Cisco Customer Experience を参照してください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 か国あまりの国々では、ハードウェア、ソフトウェア、サービス、および他社製製品を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

詳細情報

Cisco aWIPS の詳細については、https://www.cisco.com/go/aWIPS を参照してください。

Cisco DNA Center の詳細については、https://www.cisco.com/site/us/en/products/networking/index.html を参照してください。

シスコワイヤレスの詳細については、https://www.cisco.com/go/wireless を参照してください。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明箇所	日付
Cisco DNA Spaces の名称変更	製品名を Cisco Spaces に更新	10/21/22

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

0215-2023-000-X