Cisco 適応型ワイヤレス侵入防御システム コンフィギュレーション ガイド

リリース 7.2.103.0
2012 年 2 月 6 日

Text Part Number: OL-23941-02-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco 適応型ワイヤレス侵入防御システム コンフィギュレーション ガイド

CONTENTS

はじめに

ここでは、*Cisco 適応型ワイヤレス侵入防御システム*について説明します。内容は次のとおりです。

目標

このマニュアルでは、Cisco Prime Network Control System（NCS）を使用して Cisco 3300 シリーズ モビリティ サービス エンジンおよびモビリティ サービス エンジン上に常駐する Context-Aware Service を設定および管理する方法について説明します。

対象読者

このマニュアルの目的は、wIPS を設定および管理できるようにすることです。作業を開始する前に、ネットワークの構造、用語、および概念を十分に理解しておく必要があります。

表記法

このマニュアルでは、次の表記法を使用して手順および情報を表示しています。

- コマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。
- 一連のメニュー オプションは、[オプション] > [オプション] として表示されます。

例では、次の表記法を使用しています。

- 画面に表示される例およびコマンドラインは、`screen` フォントで示します。
- 入力する必要がある情報を例示する場合は、**太字の `screen` フォント**で示します。
- ユーザが値を指定する変数は、*イタリック体の `screen` フォント*で示します。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem

FONTOS BIZTONSÁGI ELOÍRÁSOK

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير **إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.
قم بحفظ هذه الإرشادات

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

関連資料

モビリティ サービス エンジンのインストールおよびセットアップ情報については、『*Cisco 3310 Mobility Services Engine Getting Started Guide or Cisco 3500 Mobility Services Engine Getting Started guide*』を参照してください。

このマニュアルは、Cisco.com の次の URL から入手可能です。

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは、現在 RSS バージョン 2.0 をサポートしています。

CHAPTER 1

概要

- この章では、Cisco Unified Wireless Network（CUWN）全体における Cisco 3300 モビリティ サービス エンジン（MSE）および Cisco Adaptive Wireless Intrusion Prevention System（wIPS）のロールについて説明します。この章は、次の内容で構成されています。
- 「wIPS について」（P.1-1）
- 「Cisco Unified Wireless Network 内の wIPS」（P.1-2）
- 「コントローラ IDS と Adaptive wIPS の違い」（P.1-6）

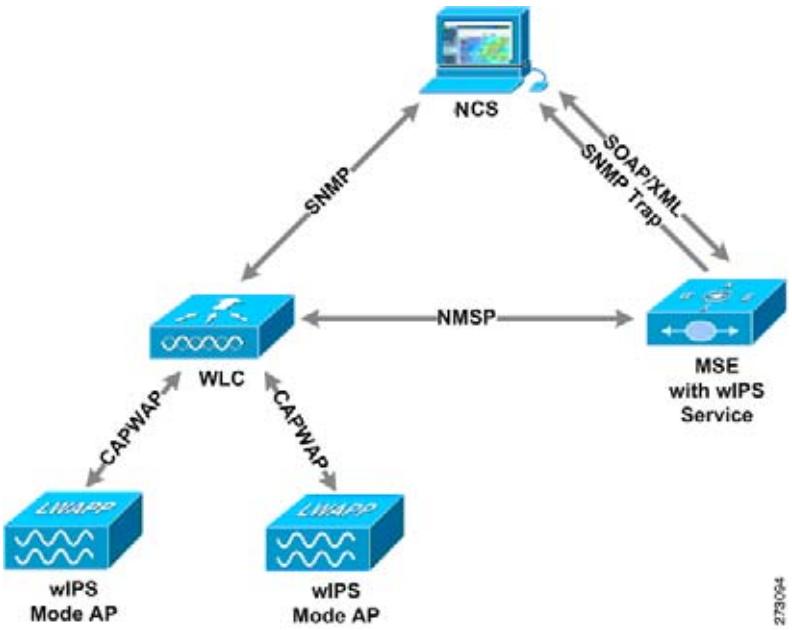
wIPS について

wIPS は、不正アクセス ポイント、不正クライアントおよびアドホック接続の検出と緩和、Over-the-Air ワイヤレス ハッキングおよび驚異の検出、セキュリティ脆弱性モニタリング、パフォーマンス モニタリングおよび自己最適化、脅威予防のためのネットワーク強化、強力なワイヤレス セキュリティ管理およびレポート作成を行います。

CUWN を基盤にし、Cisco Motion の効果を利用した wIPS は構成が強化され、企業に対応しています。wIPS は、連携して統合セキュリティ モニタリング ソリューションを実現する、次のコンポーネントで構成されています。

- wIPS ソフトウェア実行中のモビリティ サービス エンジン（MSE）：すべてのコントローラとそれぞれの wIPS モニタ モード アクセス ポイントからのアラーム集約の中央ポイント。アラーム情報とフォレンジック ファイルはアーカイブ目的でモビリティ サービス エンジンに保存されます。
- wIPS モニタ モード アクセス ポイント：攻撃検出とフォレンジック（パケット キャプチャ）機能を備えた固定チャネル スキャンを提供します。
- ローカル モード アクセス ポイント：タイムスライス型不正スキャンに加え、ワイヤレス サービスをクライアントに提供します。
- ワイヤレス LAN コントローラ：wIPS モニタ モード アクセス ポイントから受信した攻撃情報をモビリティ サービス エンジンに転送し、設定パラメータをアクセス ポイントに配布します。
- Cisco Prime Network Control System（NCS）：モビリティ サービス エンジン上での wIPS サービスの設定、コントローラへの wIPS 設定内容のプッシュ、wIPS モニタ モードのアクセス ポイントの設定を行う、一元化された管理プラットフォームを管理者に提供します。NCS は、wIPS アラーム、フォレンジック、報告の表示や、攻撃百科事典へのアクセスにも使用されます（図 1-1 を参照）。

図 1-1　Wireless Intrusion Prevention System（ワイヤレス侵入防御システム）



システム コンポーネント間の通信には、次のプロトコルが使用されます。

- Control and Provisioning of Wireless Access Points（CAPWAP）：このプロトコルは、LWAPP の後継で、アクセス ポイントとコントローラ間の通信に使用されます。これは、アラーム情報をコントローラに送信し、設定情報をアクセス ポイントに送信する双方向トンネルを提供します。
- ネットワーク モビリティ サービス プロトコル（NMSP）：このプロトコルは、コントローラとモビリティ サービス エンジン間の通信を処理します。wIPS 構成の場合、このプロトコルは、アラーム情報をコントローラから集約して、モビリティ サービス エンジンに転送し、wIPS 設定情報をコントローラに適用する経路を提供します。このプロトコルは暗号化されます。
  - コントローラ TCP ポート：16113
- Simple Object Access Protocol（SOAP/XML）：モビリティ サービス エンジンと NCS 間の通信の方法。このプロトコルは、モビリティ サービス エンジンで実行する wIPS サービスに設定パラメータを配布するために使用します。
  - MSE TCP ポート：443
- 簡易ネットワーク管理プロトコル（SNMP）：このプロトコルは、モビリティ サービス エンジンから NCS に wIPS アラーム情報を転送するために使用されます。また、コントローラから NCS に不正アクセス ポイント情報を伝えるためにも使用されます。

ガイドラインと制限事項

HREAP モード アクセス ポイントは、wIPS をサポートします。

Cisco Unified Wireless Network 内の wIPS

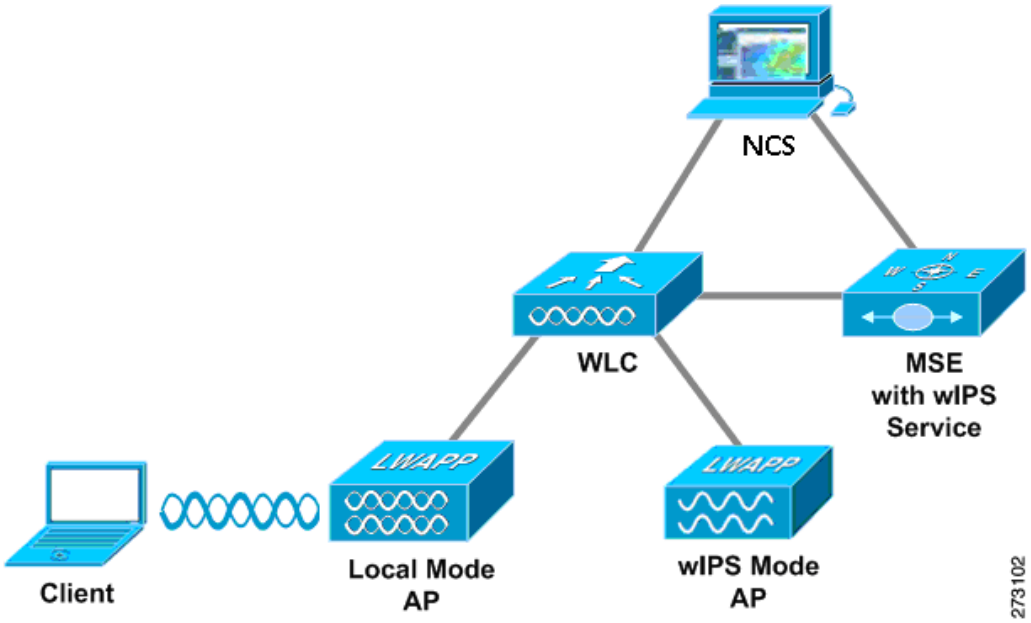
CUWN インフラストラクチャ内で wIPS を統合したり、CUWN やシスコの自律ワイヤレス ネットワーク（またはサードパーティのワイヤレス ネットワーク）に wIPS をオーバーレイしたりできます。

この項では、次のトピックを扱います。

Cisco Unified Wireless Network 内の統合された wIPS

統合 wIPS 構成は、*ローカル* モードと wIPS *モニタ モード*の両方のアクセス ポイントを同じコントローラ上で混合させ、同じ NCS によって管理するシステム設計です。これは、クライアント サービング インフラストラクチャとモニタリング インフラストラクチャ間の緊密な統合を可能にするため、推奨される構成です（図 1-2 を参照）。

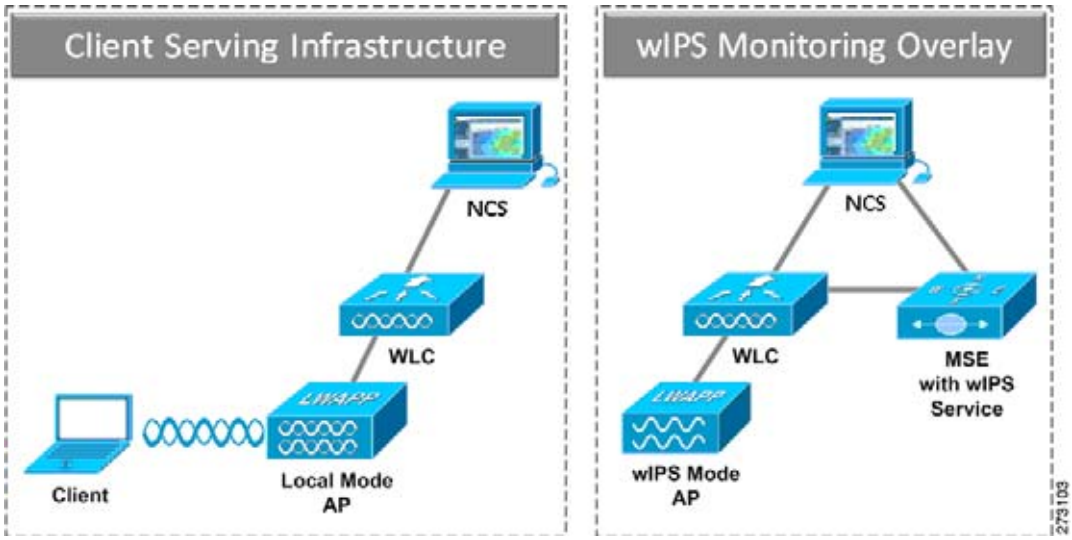
図 1-2　CUWN 内の統合された wIPS



Cisco Unified Wireless Network 内の wIPS オーバーレイ構成

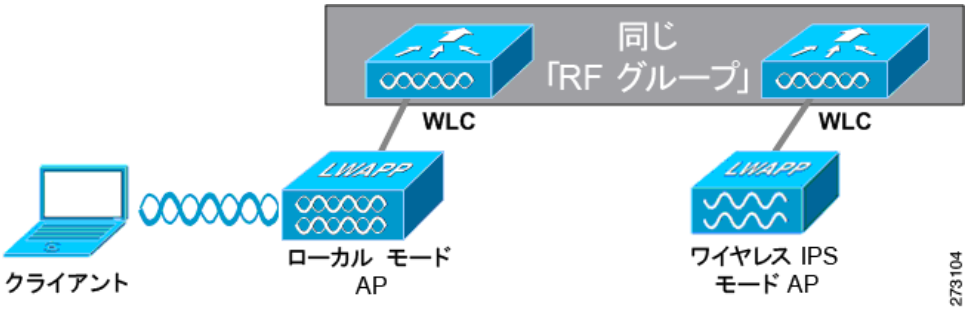
wIPS オーバーレイ構成では、wIPS モニタリング インフラストラクチャはクライアント サービング インフラストラクチャから完全に分離されます。各システムが独自のコントローラ、アクセス ポイント、および NCS のセットを使用します。この構成モデルを選択する理由の多くは、個別の管理コンソールを使用した個別のネットワーク インフラストラクチャ システムとセキュリティ インフラストラクチャ システムを必要とするビジネス上の規定に起因します（図 1-3 を参照）。また、この構成モデルは、アクセス ポイント（wIPS モニタとローカル モード）の合計数が NCS に含まれる 3000 アクセス ポイントの制限を超える場合にも使用されます。

図 1-3　CUWN 内の wIPs オーバーレイ モニタリング ネットワーク構成



wIPS オーバーレイ モニタリング ネットワークを構成して、クライアント サービング インフラストラクチャのセキュリティ査定を行うには、特定の構成項目を実行する必要があります。wIPS システムは、信頼されるデバイスに対する攻撃だけをログに記録するという前提で動作します。オーバーレイ システムで、個別の Cisco Unified WLAN インフラストラクチャを信頼されるものとして表示するには、コントローラが同じ RF グループに属している必要があります（図 1-4 を参照）。

図 1-4　wIPS オーバーレイ モニタリング ネットワークの同じ RF グループに属しているコントローラ



クライアント サービング インフラストラクチャを wIPS オーバーレイ モニタリング ネットワークから分離した結果として、いくつかのモニタリングの警告が発生します。

- wIPS アラームは、wIPS オーバーレイ NCS インスタンスにだけ表示されます。
- 管理フレーム保護（MFP）アラームは、クライアント インフラストラクチャ NCS インスタンスにだけ表示されます。
- 不正アラームは両方の NCS インスタンスに表示されます。
- 不正位置の精度は、クライアント サービング インフラストラクチャ NCS の方が高くなります。この構成では、wIPS オーバーレイ構成よりも高密度のアクセス ポイントを使用するためです。
- Over-the-Air 不正緩和は、ローカル モード アクセス ポイントを緩和操作で利用できるため、統合 wIPS モデルで拡張性が高くなります。

- セキュリティ モニタリング ダッシュボードは、両方の NCS インスタンスで不完全になります。wIPS などの一部のイベントが wIPS オーバーレイ NCS にだけ存在するためです。ワイヤレス ネットワークの包括的なセキュリティをモニタするには、両方のセキュリティ ダッシュボード インスタンスを監視する必要があります。

表 1-1 にクライアント サービング構成とオーバーレイ構成の主な相違点のいくつかを示します。

表 1-1　wIPS クライアント サービングと wIPS モニタリング オーバーレイの比較

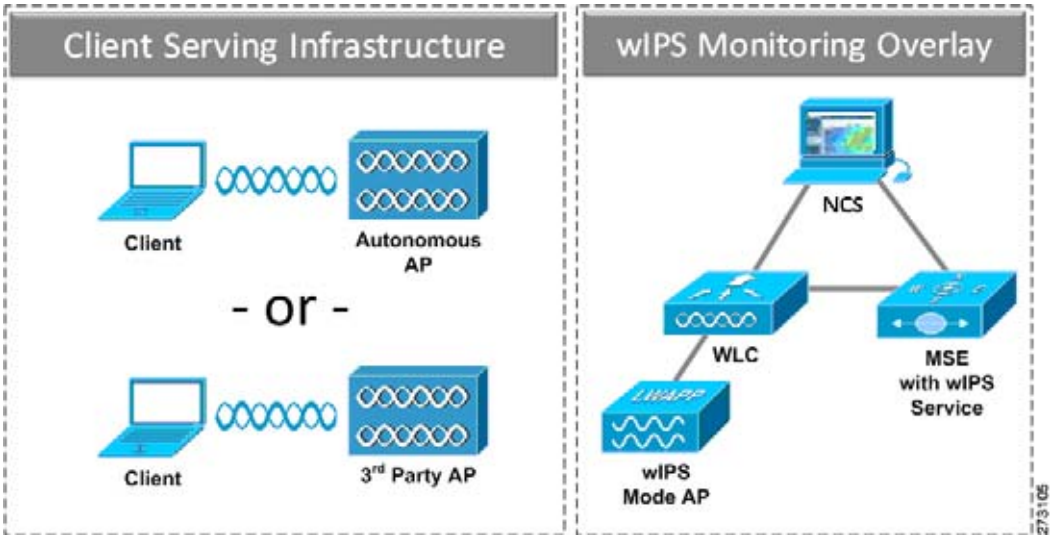
	クライアント サービング インフラストラクチャ NCS	wIPS モニタリング オーバーレイ NCS
wIPS アラーム	No	Yes
MFP アラーム	Yes	No
不正アラーム	Yes	Yes
不正位置	高精度	低精度
不正封じ込め	Yes	Yes、ただし拡張性あり

オーバーレイ ソリューションの課題の 1 つは、クライアント サービング インフラストラクチャまたは wIPS モニタリング オーバーレイ上の Lightweight アクセス ポイントが誤ったコントローラにアソシエートされる可能性です。誤ったコントローラとのアソシエーションは、各アクセス ポイント（ローカル モードと wIPS モニタ モード）で第 1、第 2、第 3 コントローラ名を指定することによって対処できます。さらに、各ソリューションのコントローラにそれぞれのアクセス ポイントとの通信用の個別の管理 VLAN を備え、アクセス コントロール リスト（ACL）を使用して CAPWAP トラフィックがこれらの VLAN 境界を超えないようにすることを推奨します。

自律ワイヤレス ネットワークまたはその他のワイヤレス ネットワークでの wIPS オーバーレイ

Adaptive wIPS ソリューションは、CUWN 以外の既存の WLAN インフラストラクチャへのセキュリティ モニタリングも実行できます。この構成の用途は、シスコの自律アクセス ポイントまたはサードパーティ アクセス ポイントのセキュリティ モニタリングです（図 1-5 を参照）。

図 1-5　自律での wIPS オーバーレイ



コントローラ IDS と Adaptive wIPS の違い

この項では、次のトピックを扱います。

ガイドラインと制限事項

フォレンジック

wIPS システムのフォレンジック機能はむやみに使用せず、目的の情報がキャプチャされたら無効にする必要があります。これは主に、アクセス ポイントにかかる負荷が大きく、スケジュールされたチャネル スキャンへの割り込みが発生するためです。wIPS アクセス ポイントでは、チャネル スキャンを実行しながら、フォレンジック ファイルを生成することはできません。フォレンジック ファイルがダンプされている間、チャネル スキャンは遅延します。

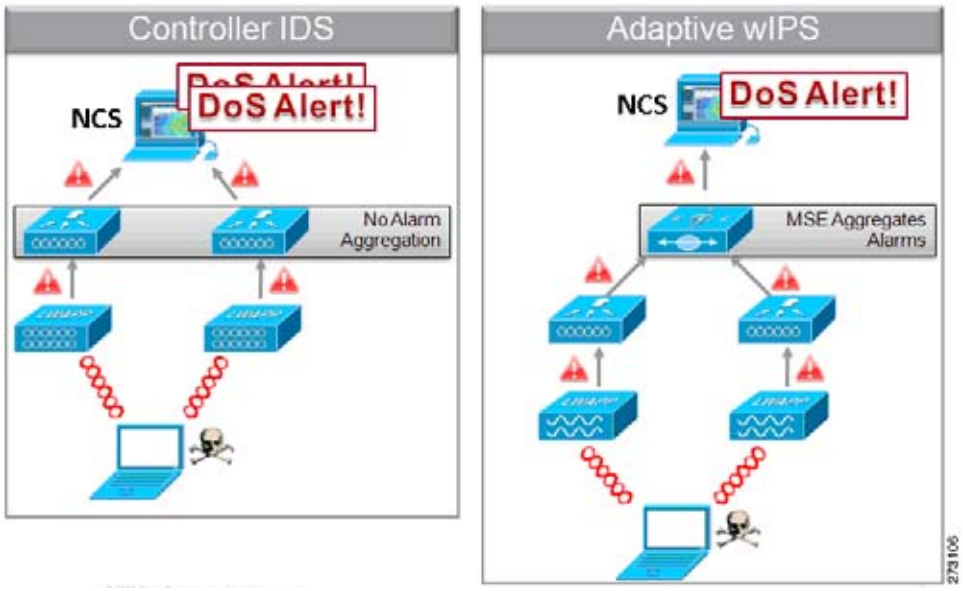
誤検出（False Positives）の削減

wIPS は、ワイヤレス ネットワークのセキュリティ モニタリングに関する誤検出を削減します。無線で多数の管理フレームを検出した場合に、アラームを生成するシスコのコントローラベースのソリューションと異なり、wIPS は、ワイヤレス インフラストラクチャ ネットワークに害を及ぼす多数の管理フレームを無線で検出した場合にだけ、アラームを生成します。これは、wIPS システムがワイヤレス インフラストラクチャ内に存在するアクセス ポイントとクライアントの状態および有効性を動的に識別できる結果です。攻撃がインフラストラクチャに対して仕掛けられた場合にだけアラームが生成されます。

アラーム集約

シスコの既存のコントローラベースの IDS システムとシスコの wIPS システムの大きな違いの 1 つは、無線で検出された一意の攻撃が 1 つのアラームに関連付けられ、集約されることです。これは、ワイヤレス IPS システムによって、特定の各攻撃が初めて識別されたときに、それらに一意のハッシュ キーを自動的に割り当てることで実行されます。複数の wIPS アクセス ポイントで攻撃が受信された場合、モビリティ サービス エンジンでアラーム集約が行われるため、攻撃は NCS に 1 回だけ転送されます。既存のコントローラベースの IDS システムはアラームを集約しません（図 1-6 を参照）。

図 1-6　シスコのコントローラベースの IDS と Adaptive wIPS を使用したアラームの集約



コントローラベースの IDS と wIPS のもう 1 つの大きな違いは、各システムで検出可能な攻撃数です。サブセクションの説明と表 1-2 および表 1-3 に示されているように、wIPS は多数の攻撃と攻撃ツールを検出できます。これらの攻撃には、サービス拒否（DoS）攻撃とセキュリティ突破攻撃の両方が含まれます。この項では、次のトピックを扱います。

- 「DoS 攻撃」（P.1-8）。
- 「セキュリティ突破攻撃」（P.1-8）
- 「ワイヤレス IPS アラーム フロー」（P.1-9）

DoS 攻撃

DoS 攻撃には、ワイヤレス ネットワーク内の正常な通信を妨害または遅延させるように設計されたメカニズムが含まれます。これらには、ワイヤレス ネットワーク内の正規の接続をドロップさせたり、不安定にさせるように設計された多数のスプーフされたフレームが組み込まれることがあります。DoS 攻撃は、ワイヤレス ネットワークの信頼できるサービスを提供する機能に打撃を与える可能性がありますが、データ違反にはならず、攻撃が停止すれば、多くの場合マイナスの影響はなくなります。表 1-2 に、コントローラベースの IDS と wIPS サービスで検出される Dos 攻撃の比較を示します。

表 1-2　コントローラ IDS と wIPS によって検出される DoS 攻撃

アラーム名	コントローラ IDS によって検出	ワイヤレス IPS によって検出
アソシエーション フラッド	○	○
アソシエーション テーブル オーバーフロー		○
認証フラッド	○	○
EAPOL-Start 攻撃	○	○
PS-Poll フラッド		○
認証されないアソシエーション		○
CTS フラッド		○
クイーンズランド工科大学により検出された脆弱性		○
RF 電波妨害攻撃		○
RTS フラッド		○
仮想キャリア攻撃	○	○
認証失敗攻撃		○
認証解除ブロードキャスト攻撃	○	○
認証解除フラッド攻撃	○	○
ディスアソシエーション ブロードキャスト攻撃		○
ディスアソシエーション フラッド攻撃	○	○
EAPOL-Logoff 攻撃	○	○
FATA-jack ツールの検出		○
不完全な EAP-failure 攻撃		○
不完全な EAP-success attack		○

セキュリティ突破攻撃

ワイヤレス ネットワークを脅かす 2 つの攻撃タイプのうち、ほぼ間違いなく有害性の高いセキュリティ突破は、機密データや後で機密データを見るために使用できる暗号キーなどの情報をキャプチャしたり、公開したりするように設計されています。セキュリティ突破攻撃には、インフラストラクチャに対するクエリや暗号キーを解読することを目的とした応答攻撃が含まれることがあります。さらに、セキュリティ突破攻撃は、ハニーポットなどの疑似アクセス ポイントにクライアントの誘導を試みることによってクライアントに害を及ぼす可能性もあります。表 1-3 に、コントローラベースの IDS と wIPS サービスで検出されるセキュリティ突破攻撃の比較を示します。

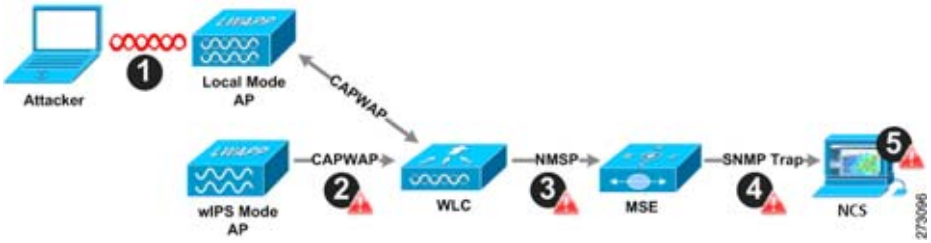
表 1-3　コントローラ IDS と wIPS によって検出されるセキュリティ突破攻撃

アラーム名	コントローラ IDS によって検出	ワイヤレス IPS によって検出
Airsnarf 攻撃		○
ChopChop 攻撃		○
WLAN のセキュリティ異常による Day-Zero 攻撃		○
デバイスのセキュリティ異常による Day-Zero 攻撃		○
アクセス ポイントのデバイス プローブ		○
EAP メソッドへの辞書攻撃		○
802.1x 認証に対する EAP 攻撃		○
疑似アクセス ポイントの検出	○	○
偽の DHCP サーバの検出		○
高速 WEP クラックの検出		○
フラグメンテーション攻撃		○
Hotspotter ツールの検出		○
不正 802.11 パケットの検出		○
中間者攻撃の検出		○
NetStumbler の検出	○	○
PSPF 違反		○
ASLEAP 攻撃の検出		○
ハニーポット アクセス ポイントの検出	○	○
ソフト アクセス ポイントまたはホスト アクセス ポイントの検出		○
スプーフされた MAC アドレスの検出		○
疑わしい営業時間外のトラフィック		○
ベンダー リストによる未承認アソシエーション		○
未承認アソシエーションの検出		○
Wellenreiter の検出	○	○

ワイヤレス IPS アラーム フロー

Adaptive wIPS システムは、通信のリニア チェーンに従って、エアウェーブの初期スキャンから取得した攻撃情報を伝播して、情報を NCS に転送します（図 1-7 を参照）。

図 1-7　ネットワーク内のアラーム フロー



1. wIPS システムでアラームを生成させるには、正規のアクセス ポイントまたはクライアントに対して攻撃が仕掛けられる必要があります。正規のアクセス ポイントおよびクライアントは、同じ RF グループ名をブロードキャストする信頼するデバイスによって、CUWN 内で自動的に検出されます。この設定では、ローカルモード アクセス ポイントとそれらにアソシエートされたクライアントのリストが動的に管理されます。SSID グループ機能を使用して、SSID によってデバイスを信頼するようにシステムを設定することもできます。WLAN インフラストラクチャに害を及ぼすと見なされた攻撃だけが残りのシステムに伝播されます。
2. wIPS モニタ モード アクセス ポイントによって攻撃が識別されると、アラームの更新がコントローラに送信され、CAPWAP 制御トンネル内にカプセル化されます。
3. コントローラは、アラームの更新をアクセス ポイントから、モビリティ サービス エンジンを実行する wIPS サービスに透過的に転送します。この通信に使用されるプロトコルは Network Mobility Service Protocol（NMSP）です。
4. モビリティ サービス エンジン上の wIPS サービスが受信したアラームの更新は、アーカイブと攻撃の追跡のためにアラーム データベースに追加されます。SNMP トラップが NCS に転送されます。SNMP トラップには攻撃情報が含まれています。同じ攻撃を参照する複数のアラーム更新を受信した場合（たとえば、複数のアクセス ポイントで同じ攻撃が認識された）、1 つの SNMP トラップだけが NCS に送信されます。
5. アラーム情報を含む SNMP トラップは NCS によって受信され、表示されます。

フォレンジック

Cisco Adaptive wIPS システムは、詳しい調査とトラブルシューティングの目的で、攻撃フォレンジックをキャプチャする機能を提供します。基本レベルでは、フォレンジック機能は、一連のワイヤレス フレームをログに記録し、取得する切り替えベースのパケット キャプチャ ファシリティです。この機能は、wIPS プロファイル内で、攻撃単位で有効になります。wIPS プロファイルは NCS 上に設定されます。

この機能を有効にすると、エアウェーブで特定の攻撃アラームが確認されると、フォレンジック機能がトリガーされます。元のアラームを生成した wIPS モニタ モード アクセス ポイントのバッファ内に格納されたパケットに基づいて、フォレンジック ファイルが作成されます。このファイルは CAPWAP によってコントローラに転送されます。次に、この CAPWAP によって、NMSP 経由でフォレンジック ファイルが、モビリティ サービス エンジンで実行されている wIPS に転送されます。このファイルは、ユーザがフォレンジックに設定したディスク容量制限に達するまで、モビリティ サービス エンジンのフォレンジック アーカイブに保存されます。デフォルトでは、この制限は 20 GB で、この制限に達すると、最も古いフォレンジック ファイルが削除されます。フォレンジック ファイルには、フォレンジック ファイルへのハイパーリンクを含むアラームを NCS で開くことでアクセスできます。このファイルは、a.CAP ファイル形式で保存されており、WildPacket Omnipeek、AirMagnet WiFi Analyzer、Wireshark、またはこの形式をサポートしているその他のパケット キャプチャ プログラムを使用してアクセスできます。Wireshark は、http://www.wireshark.org から入手できます。

（注）　wIPS システムのフォレンジック機能はむやみに使用せず、目的の情報がキャプチャされたら無効にする必要があります。これは主に、アクセス ポイントにかかる負荷が大きく、スケジュールされたチャネル スキャンへの割り込みが発生するためです。wIPS アクセス ポイントでは、チャネル スキャンを実行しながら、フォレンジック ファイルを生成することはできません。フォレンジック ファイルがダンプされている間、チャネル スキャンは遅延します。

不正検出

wIPS に最適化されたモニタ モードのアクセス ポイントは、現在の CUWN 実装と同じロジックを使用して、不正の脅威の査定と緩和を行います。これにより、ワイヤレス IPS モード アクセス ポイントは、不正アクセス ポイントおよびアドホック ネットワークをスキャンし、検出して、封じ込めることができます。不正ワイヤレス デバイスに関するこの情報が発見されると、不正アラーム集約が行われる NCS に報告されます。

ただし、この機能を使用すると、ワイヤレス IPS モード アクセス ポイントを使用して、攻撃封じ込めが起動された場合、封じ込めの間、系統的な攻撃を狙いとしたチャネル スキャンを実行する機能が中断されます。

異常検出

wIPS には、キャプチャされた攻撃パターンやデバイス特性の異常性に関する特定のアラームが含まれます。異常検出システムでは、モビリティ サービス エンジン内に格納された攻撃履歴ログおよびデバイス履歴を考慮して、ワイヤレス ネットワークの一般的な特性の基準を定めます。システム上のイベントまたは攻撃に、モビリティ サービス エンジンに保存されている履歴データと比較して、ある程度の変化が見られた場合に、異常検出エンジンがトリガーされます。たとえば、システムで毎日わずかな MAC スプーフィング イベントを定期的にキャプチャしており、別の日に MAC スプーフィング イベントが 200 % 増加した場合、そのモビリティ サービス エンジンで異常アラームがトリガーされます。次に、このアラームが NCS に送信され、システムで発生する可能性のある従来の攻撃を超えた何かがワイヤレス ネットワークで発生していることが管理者に通知されます。さらに、異常検出アラームは、wIPS システムに既存のシグニチャがない可能性のある Day-Zero 攻撃を検出するためにも使用できます。

デフォルトの設定プロファイル

特定の各 WLAN セキュリティ構成に合わせた設定の調整を容易にするため、wIPS には、特定の産業や導入のセキュリティ ニーズに合わせて作られた多数のデフォルトのプロファイルが用意されています。テンプレートには、さまざまなリスク プロファイルおよび導入ごとに異なるセキュリティ モニタリングの要件が要約されています。特定のプロファイルには、Education、Enterprise（Best）、Enterprise（Rogue）、Financial、Healthcare、Hotspot（Open Security）、Hotspot（802.1x Security）、Military、Retail、Tradeshow、Warehouse などがあります。プロファイルは、目的の構成の特定のニーズに合わせてさらにカスタマイズできます。

リリース 7.0 機能への統合

wIPS は、以前のリリースで導入されたセキュリティ機能を利用するために、既存の CUWN に緊密に統合されます。セキュリティ ダッシュボードでは、それぞれのカテゴリの下に wIPS イベントが表示されます。

設定と管理

NCS を使用して、モビリティ サービス エンジンの追加と削除、モビリティ サービス エンジン プロパティの設定、ユーザとグループの管理をはじめとした、さまざまな設定タスクと管理タスクを実行できます。

この項では、次のトピックを扱います。

モビリティ サービス エンジンの追加と削除

NCS を使用して、ネットワーク内のモビリティ サービス エンジンの追加と削除ができます。モビリティ サービス エンジンでサポートされているサービスを定義することもできます。設定の詳細については第 2 章「モビリティ サービス エンジンとライセンスの追加および削除」を参照してください。

モビリティ サービス エンジンの同期

NCS を使用して、Cisco Wireless LAN Controllers と NCS をモビリティ サービス エンジンと同期できます。詳細については、第 3 章「モビリティ サービス エンジンの同期」を参照してください。

ハイ アベイラビリティの設定

NCS を使用して、MSE にハイ アベイラビリティを設定できます。モビリティ サービス エンジンは、複数のモビリティ アプリケーションをホストするプラットフォームです。アクティブな各 MSE は別の非アクティブ インスタンスによりバックアップされます。アクティブな MSE はプライマリ MSE、非アクティブな MSE はセカンダリ MSE と呼ばれます。詳細については、第 4 章「ハイ アベイラビリティの設定」を参照してください。

仮想アプライアンスの設定

MSE は、さまざまなパフォーマンス特性を持つ物理アプライアンスにプリインストールされます。MSE は、物理アプライアンスと仮想アプライアンスの 2 つのモードで提供されます。詳細については、第 5 章「MSE 配信モード」を参照してください。

モビリティ サービス エンジンのプロパティの編集

NCS を使用して、モビリティ サービス エンジンの次のパラメータを設定できます。設定の詳細については第 6 章「システム プロパティの設定および表示」を参照してください。

- [General Properties]：連絡先名、ユーザ名、パスワード、およびモビリティ サービス エンジンの HTTP を割り当てることができます。
- [Active Sessions]：モビリティ サービス エンジン上のアクティブなユーザ セッションを確認できます。
- [Trap Destinations]：モビリティ サービス エンジンにより生成される SNMP トラップを受信する NCS または Cisco Security Monitoring, Analysis, and Response System（CS-MARS）ネットワーク管理プラットフォームを指定できます。
- [Advanced Parameters]：イベントを保存する日数、ハードウェアのリブート、ハードウェアのシャットダウン、またはデータベースのクリアの設定ができます。

ユーザとグループの管理

NCS を使用して、ユーザ、グループ、およびモビリティ サービス エンジンへのホスト アクセスを管理できます。設定の詳細については第 7 章「ユーザとグループの管理」を参照してください。

wIPS の設定およびプロファイル管理

NCS を使用して、Cisco Adaptive wIPS サービスを設定できます。詳細については、「wIPS プロファイルの設定」（P.8-4）を参照してください。

モニタリング機能

NCS を使用して、モビリティ サービス エンジンによって生成されるアラーム、イベント、およびログをモニタできます。モビリティ サービス エンジンのステータス、クライアント、干渉、タグ付きアセットもモニタできます。また、モビリティ サービス エンジンの使用率レポートを生成して、CPU とメモリの使用率を判断し、クライアント、タグ、および不正アクセス ポイントと不正クライアントをカウントすることができます。詳細については、第 9 章「システムとサービスのモニタリング」を参照してください。

MSAP 要件のプロビジョニング

Cisco Mobility Services Advertisement Protocol（MSAP）では、MSAP クライアントおよびサーバの要件を規定し、それらの間でのメッセージ交換を記述します。モバイルデバイスは、MSAP を使用して MSAP サーバから Wi-Fi インフラストラクチャを介してサービス アドバタイズメントを取得できます。このリリースのモビリティ サービス エンジン（MSE）では、MSAP が導入され、サーバ機能が提供されています。詳細については、第 10 章「MSAP」を参照してください。

メンテナンス操作

NCS に事前に定義した FTP フォルダにモビリティ サービス エンジンのデータを定義した間隔でバックアップし、その NCS からモビリティ サービス エンジンのデータを復元することができます。その他の実行できるモビリティ サービス エンジンのメンテナンス操作には、NCS ステーションからアソシエートされているすべてのモビリティ サービス エンジンへの新規ソフトウェア イメージのダウンロード、モビリティ サービス エンジンの設定のクリアなどがあります。詳細については、第 11 章「メンテナンス操作の実行」を参照してください。

（注）　NCS の代わりに、コマンドライン インターフェイスを使用して、モビリティ サービス エンジンの GRUB とルート パスワードを復元する方法の詳細については、第 11 章「メンテナンス操作の実行」も参照してください。

MSE システムとアプライアンスの強化

システムとアプライアンスを強化するには、正常に機能させるために一部のサービスとプロセスを公開する必要があります。MSE の強化には、不要なサービスの無効化、最新のサーバ バージョンへのアップグレード、ファイル、サービス、エンド ポイントへの適切な制限付き権限の適用が含まれます。

システム互換性

現在使用しているリリースに対する最新システム（コントローラ、NCS、モビリティ サービス エンジン）の互換性情報、機能のサポート、および操作上の注意については、次の URL で入手可能な『Cisco 3300 Mobility Services Engine Release Note』を参照してください。
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

CHAPTER 2

モビリティ サービス エンジンとライセンスの追加および削除

この章では、Cisco 3300 シリーズ モビリティ サービス エンジンを Cisco NCS に対して追加および削除する方法について説明します。

この章は、次の内容で構成されています。

MSE のライセンス要件

MSE には、次のような関連サービス エンジンとアプリケーション プロセスとともに、ネットワーク トポロジ、NMSP などの設計、ネットワーク リポジトリに関連する複数の製品機能が付属しています。

- ロケーション サービスまたは Context-Aware Service ソフトウェア
- ワイヤレス侵入防御システム（wIPS）

MSE とそのサービスをスムーズに管理できるように、各種ライセンスが提供されています。

この項では、次のトピックを扱います。

MSE ライセンスの構成マトリクス

表 2-1 に、MSE、ロケーション サービスまたは Context-Aware Service ソフトウェア、および wIPS について、ハイエンド、ローエンド、および評価ライセンスのライセンス内容を示します。

表 2-1　MSE ライセンスの構成マトリクス

	ハイエンド	ローエンド	評価
MSE プラットフォーム	ハイエンド アプライアンスおよびインフラストラクチャ プラットフォーム	ローエンド アプライアンスおよびインフラストラクチャ プラットフォーム	60 日間
ロケーション サービスまたは Context-Aware Service ソフトウェア	3000、6000、12,000 タグ	1000 タグ	60 日間、100 タグおよび 100 要素
	3000、6000、12,000 要素	1000 要素	
wIPS	5000 アクセス ポイント	2000 アクセス ポイント	60 日間、20 アクセス ポイント

MSE ライセンス ファイルのサンプル

次に、MSE ライセンス ファイルのサンプルを示します。

```
FEATURE MSE cisco 1.0 permanent uncounted \
        VENDOR_STRING=UDI=udi,COUNT=1 \
        HOSTID=ANY \
        NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</Li cLineID> \
        <PAK>dummyPak</PAK>" \
        SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
        45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
        1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

このサンプル ファイルには、ライセンス エントリが 5 つあります。どのライセンス エントリでも最初の行の先頭の語は、どのタイプのライセンスであるかを示します。これは、Feature または Increment ライセンスのいずれかになります。Feature（機能）ライセンスは、単一アイテムの固定ライセンスです。複数のサービス エンジンを MSE で実行できます。Increment（増分）ライセンスは、追加型のライセンスです。MSE では、個々のサービス エンジンが Increment ライセンスとして扱われます。

最初の行の 2 番めの語は、ライセンス付与する特定のコンポーネントを定義します。たとえば、MSE です。3 番めの語はライセンスのベンダーを示します。たとえば、Cisco などです。4 番めの語はライセンスのバージョンを示します。たとえば、1.0 などです。5 番めの語は有効期限を示します。これは、期限のないライセンスの場合は permanent、それ以外の場合は dd-mmm-yyyy の形式の日付になります。最後の語は、このライセンスをカウントするかどうかを定義します。

MSE ライセンスの取り消しと再使用

MSE アプリケーション ライセンスをあるシステムから取り消し、別のシステムで再使用できます。ライセンスを取り消すと、ライセンス ファイルはシステムから削除されます。ライセンスを別のシステムで再使用する場合は、ライセンスをリホストする必要があります。

別のシステムでアップグレード SKU を使用してライセンスを再使用する場合は、対応する Base ライセンス SKU を、アップグレード SKU を再使用するシステムにインストールする必要があります。対応する Base ライセンス SKU がシステムから削除された場合、そのシステムではアップグレード ライセンス SKU を再使用できません。

ライセンスを取り消すと、ライセンスに対して変更を反映するため、MSE により個別のサービス エンジンが再起動されます。次に、サービス エンジンは、起動時に MSE から更新された容量を受け取ります。

ライセンスの詳細については、『*Cisco Prime Network Control System Configuration Guide, Release 7.0.x*』を参照してください。

MSE CLI を使用した MSE ライセンスの取り消し

NCS を使用せずに、MSE コマンドライン インターフェイスから手動で MSE ライセンスを取り消すこともできます。

MSE コマンドライン インターフェイスを使用して MSE ライセンスを取り消すには、次の手順に従います。

ステップ 1　コマンドライン インターフェイスを使用して MSE にログインします。

ステップ 2　/opt/mse/licensing/ に移動します。

ステップ 3　次のコマンドを入力して、ライセンス ファイルを削除します。

rm /opt/mse/licensing/*license file name*.**lic**

license file name はライセンス ファイルの名前です。

ステップ 4　次のコマンドを入力して、MSE プロセスを再開します。

/etc/init.d/msed restart

MSE ライセンスが取り消されました。

ガイドラインと制限事項

MSE を NCS に追加し、デバイスおよび wIPS 製品認証キーを登録する場合、次のガイドサインに従います。

- モビリティ サービス エンジンは複数のサービスをサポートできます。
- 新しいモビリティ サービス エンジンを追加すると、ネットワーク設計（キャンパス、ビルディング、および屋外マップ）、コントローラ、スイッチ（Catalyst 3000 シリーズおよび 4000 シリーズのみ）、およびモビリティ サービス エンジンのイベント グループと NCS を同期できます。
- タグ PAK は、MSE の追加時にタグの AeroScout エンジンが選択された場合にだけ AeroScout に登録します。シスコ ライセンスとして選択されたシスコ タグ エンジンがタグを含むすべてのデバイスで共有される場合、この手順は必要ありません。
- 自動インストール スクリプトの実行中にユーザ名とパスワードを変更した場合は、モビリティ サービス エンジンを NCS に追加する際に変更後の値をここで入力します。デフォルト パスワードを変更しなかった場合は、自動インストール スクリプトを再実行してユーザ名とパスワードを変更することを推奨します。

モビリティ サービス エンジンの NCS への追加

[Mobility Service] ページの [Add Mobility Services Engine] ダイアログボックスを使用して MSE を追加できます。このダイアログボックスでは、ライセンス ファイルと追跡パラメータを追加し、マップを MSE に割り当てることができます。設定のために既存の MSE でウィザードを起動する場合、[Add MSE] オプションの代わりに [Edit MSE Details] として表示されます。

ヒント　Cisco Adaptive wIPS 機能の詳細については、Cisco.com でマルチメディア プレゼンテーションを参照してください。NCS に関するさまざまなトピックについての学習モジュールがあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

（注）　NCS Release 1.0 は MSE 3355 を認識し、適切にサポートしています。

モビリティ サービス エンジンを NCS に追加するには、NCS にログインし、次の手順に従います。

ステップ 1　モビリティ サービス エンジンに対して ping を実行できることを確認します。

ステップ 2　[Services] > [Mobility Services] の順に選択し、[Mobility Services] ページを表示します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Mobility Services Engine] を選択します。[Go] をクリックします。

ステップ 4　[Device Name] テキスト ボックスに、モビリティ サービス エンジンの名前を入力します。

ステップ 5　[IP Address] テキスト ボックスに、モビリティ サービス エンジンの IP アドレスを入力します。

ステップ 6　（任意）[Contact Name] テキスト ボックスに、モビリティ サービス エンジン管理者の名前を入力します。

ステップ 7　[User Name] および [Password] テキスト ボックスに、モビリティ サービス エンジンのユーザ名とパスワードを入力します。

これは、設定時に作成された NCS 通信ユーザ名とパスワードです。

設定時にユーザ名とパスワードを指定しなかった場合は、デフォルトを使用します。

デフォルトのユーザ名とパスワードはどちらも *admin* です。

（注）　自動インストール スクリプトの実行中にユーザ名とパスワードを変更した場合は、変更後の値をここに入力してください。デフォルト パスワードを変更しなかった場合は、自動インストール スクリプトを再実行してユーザ名とパスワードを変更することを推奨します。

ステップ 8　[HTTP] チェックボックスをオンにして、モビリティ サービス エンジンとサードパーティ アプリケーションの間の通信を許可します。デフォルトでは、NCS は MSE との通信に HTTPS を使用します。

ステップ 9　モビリティ サービス エンジンからすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。

このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 10　[Next] をクリックします。NCS により、選択されている要素と MSE が自動的に同期されます。

同期完了後、[MSE License Summary] ページが表示されます。[MSE License Summary] ページから、ライセンスのインストール、ライセンスの追加、ライセンスの削除、アクティベーション ライセンスのインストール、サービス ライセンスのインストールを実行できます。[Select Mobility Service] ページが表示されます。

ステップ 11　モビリティ サービス エンジン上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。サービスには Context-Aware Service および wIPS が含まれます。

CAS を選択すると、クライアント、不正アクセス ポイント、干渉、有線クライアント、およびタグを追跡できます。

タグを追跡するには、次のいずれかのエンジンを選択します。

- Cisco Tag Engine

  または

- Partner Tag Engine

ステップ 12　[Save] をクリックします。

（注）　第 3 章「モビリティ サービス エンジンの同期」を参照してください。

（注）　新しいモビリティ サービス エンジンを追加すると、NCS を使用して、ネットワーク設計（キャンパス、ビルディング、および屋外マップ）、コントローラ、スイッチ（Catalyst シリーズ 3000 のみ）、およびローカル モビリティ サービス エンジンのイベント グループを同期できます。この同期は、新しいモビリティ サービス エンジンを追加した直後、または後で実行できます。ローカル データベースと NCS データベースを同期するには、第 3 章「モビリティ サービス エンジンの同期」を参照してください。

モビリティ サービス エンジンでのサービスの有効化

ステップ 1　ライセンス ファイルを追加すると、[Select Mobility Service] ページが表示されます。

ステップ 2　モビリティ サービス エンジン上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。サービスのタイプは次のとおりです。

- [Context Aware Service] : [Context Aware Service] チェックボックスをオンにすると、ロケーション計算を実行するためにロケーション エンジンを選択する必要があります。CAS を選択すると、**クライアント**、**不正アクセス ポイント**、**干渉**、および**タグ**を追跡できます。タグを追跡するには、次のいずれかのエンジンを選択します。
  - Cisco Context-Aware Engine for Clients and Tags
  - Partner Tag Engine

  （注）　デフォルトで、[Context Aware Service] チェックボックスおよび [Cisco Context-Aware Engine for Clients and Tags] オプション ボタンはオンになっています。

- [Wireless Intrusion Prevention System] : [Wireless Intrusion Prevention System] チェックボックスをオンにすると、無線およびパフォーマンスの脅威が検出されます。
- [MSAP Service] : [MSAP Service] チェックボックスをオンにすると、モバイル デバイスで使用可能なサービスが記述されるサービス アドバタイズメントが提供されます。

（注）　MSE 6.0 以降では、複数のサービス（CAS と wIPS）を同時に有効にできます。6.0 よりも前のバージョンでは、モビリティ サービス エンジンでは一度に 1 つのアクティブ サービスだけがサポートされていました。

ステップ 3　[Next] をクリックして、追跡パラメータを設定します。

MSE 追跡パラメータおよび履歴パラメータの設定

ステップ 1　モビリティ サービス エンジンでサービスを有効にすると、[Select Tracking & History Parameters] ページが表示されます。

（注）　追跡パラメータの設定を省略すると、デフォルト値が選択されます。

ステップ 2　追跡するクライアントを選択するには、対応する [Tracking] チェックボックスをオンにします。追跡パラメータを以下に示します。

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

ステップ 3　デバイスの履歴トラッキングを有効にするには、対応するデバイスのチェックボックスをオンにします。履歴パラメータを以下に示します。

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

ステップ 4　[Next] をクリックして MSE にマップを割り当てます。

MSE へのマップの割り当て

（注）　[Assigning Maps] ページは、MSE で有効にするサービスの 1 つとして CAS を選択する場合にだけ使用可能です。

ステップ 1　MSE 追跡パラメータおよび履歴パラメータを設定すると、[Assigning Maps] ページが表示されます。

[Assign Maps] ページには以下の情報が表示されます。

- Map Name
- [Type]（ビルディング、フロア、キャンパス）
- Status

ステップ 2　必要なマップ タイプを確認するには、ページで使用可能な [Filter] オプションから [All]、[Campus]、[Building]、[Floor Area]、または [Outdoor Area] を選択します。

ステップ 3　マップを同期するには、[Name] チェックボックスをオンにし、[Synchronize] をクリックします。

ネットワーク設計の同期が完了すると、特定のネットワーク設計で AP が割り当てられている適切なコントローラが MSE と自動的に同期されます。[Done] をクリックして MSE 設定を保存します。

NCS からのモビリティ サービス エンジンの削除

NCS データベースから 1 つ以上のモビリティ サービス エンジンを削除するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

[Mobility Services] ページが表示されます。

ステップ 2　削除するモビリティ サービス エンジンを選択するため、対応する [Device Name] チェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Delete Service(s)] を選択します。[Go] をクリックします。

ステップ 4　選択したモビリティ サービス エンジンを NCS データベースから削除することを確定するには、[OK] をクリックします。

ステップ 5　削除を中止するには、[Cancel] をクリックします。

デバイスと wIPS 製品認証キーの登録

CAS 要素、wIPS、またはタグのライセンスをシスコに発注すると、製品認証キー（PAK）が配布されます。モビリティ サービス エンジン上にインストールするライセンス ファイルを受け取るには、PAK を登録する必要があります。PAK の登録に成功すると、ライセンス ファイルが電子メールで送信されます。

クライアントおよびワイヤレス IPS の PAK は、シスコに登録します。

（注）　詳細については、「タグ PAK の登録」（P.2-11）を参照してください。

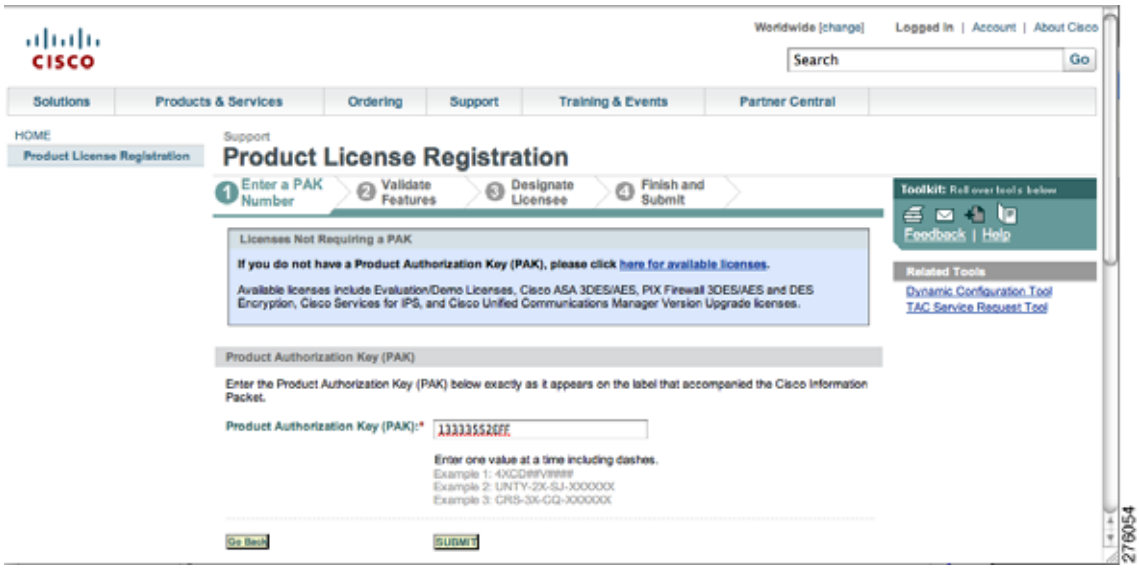
インストールするライセンス ファイルを入手するために PAK を登録するには、次の手順に従います。

ステップ 1　ブラウザ ページを開いて、次の URL を入力します。

https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet

ステップ 2　PAK を入力し、[SUBMIT] をクリックします（図 2-1 を参照）。

図 2-1　[Enter PAK Number] ページ



ステップ 3　ライセンスの購入内容を確認します。正しい場合は [Continue] をクリックします（図 2-2 を参照）。ライセンス入力ページが表示されます（図 2-3 を参照）。

（注）　ライセンスが正しくない場合は、[TAC Service Request Tool] URL をクリックして問題をレポートしてください。

図 2-2　[Validate Features] ページ

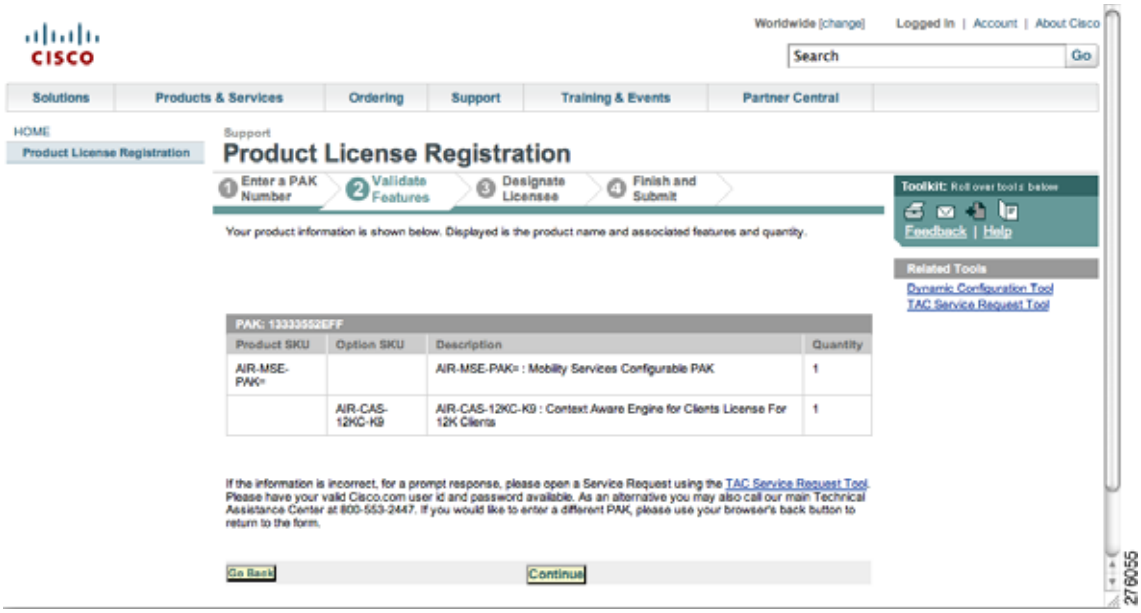
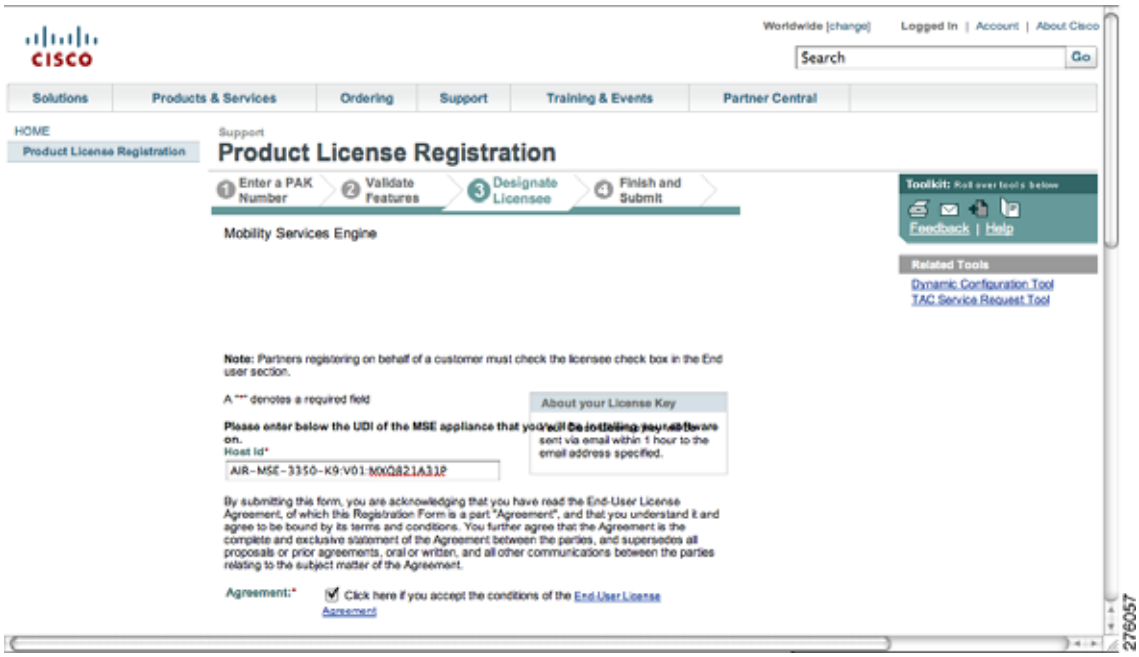


図 2-3　[Designate Licensee]（1/2 ページ）

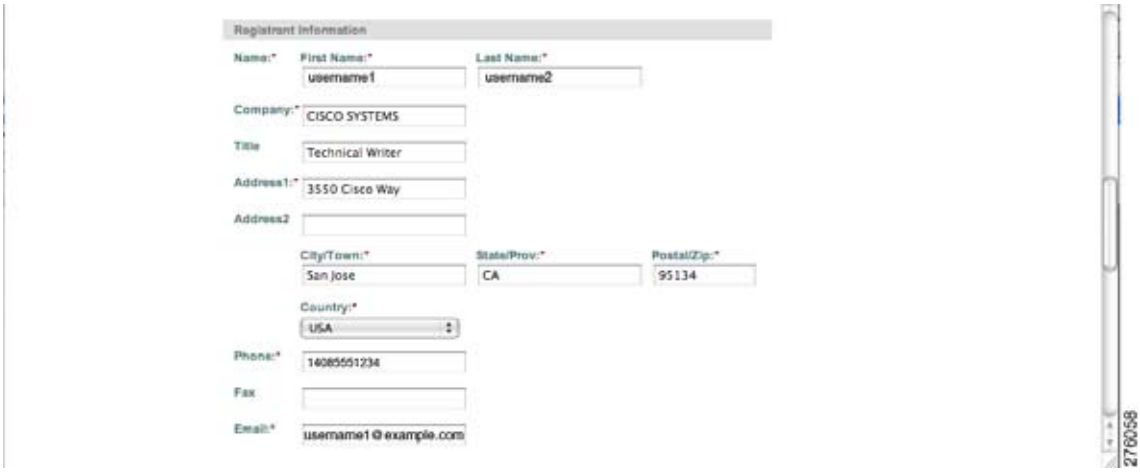


ステップ 4　[Designate Licensee] ページで、[Host Id] テキスト ボックスにモビリティ サービス エンジンの UDI を入力します。これは、ライセンスがインストールされているモビリティ サービス エンジンです。

（注）　モビリティ サービス エンジンの UDI 情報は、[Services] > [Mobility Services Engine] > *デバイス名* > *システム* の [General Properties] に表示されます。

ステップ 5　[Agreement] チェックボックスをオンにします。[Agreement] チェックボックスの下に登録者情報が表示されます（図 2-4 を参照）。

図 2-4　[Designate Licensee]（2/2 ページ）

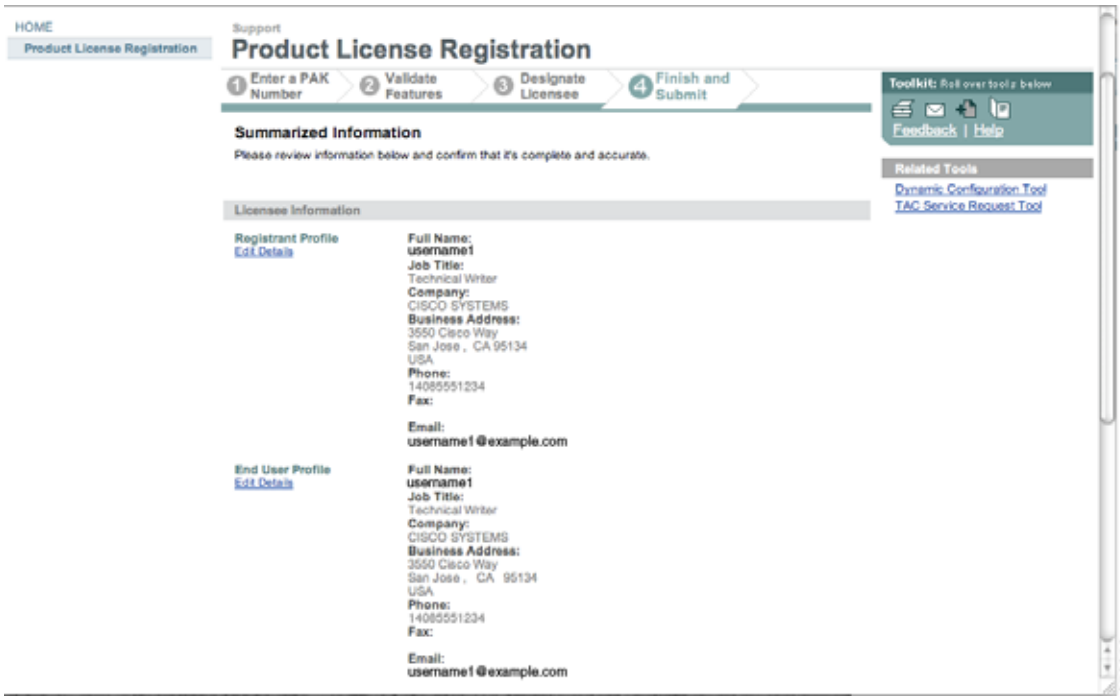


必要に応じて情報を変更します。

ステップ 6　登録者とエンド ユーザが異なる場合は、登録者情報の下の [Licensee (End-User)] チェックボックスをオンにしてエンド ユーザ情報を入力します。

ステップ 7　[Continue] をクリックします。入力したデータの概要が表示されます（図 2-5 を参照）。

図 2-5　[Finish and Submit] ページ



ステップ 8　[Finish and Submit] ページで、登録者データとエンド ユーザ データを確認します。情報を訂正するには、[Edit Details] をクリックします。[Submit] をクリックします。確認ページが表示されます（図 2-6 を参照）。

図 2-6　登録確認ページ

デバイスおよび wIPS ライセンス ファイルのインストール

NCS からクライアント ライセンスと wIPS ライセンスをインストールできます。

（注）　タグ ライセンスのインストールは、MSE の追加時に AeroScout エンジンがタグ計算用に選択されている場合に限り別途行います。

タグ ライセンスをインストールするには、AeroScout System Manager を使用します。詳細については、「タグ ライセンスのインストール」（P.2-12）を参照してください。

PAK の登録後にクライアント ライセンスまたは wIPS ライセンスを NCS に追加するには、次の手順に従います。

ステップ 1　[Administration] > [License Center] を選択します。

図 2-7　[Administration] > [License Center] ページ

ステップ 2　左側のサイドバーのメニューから、[Files] > [MSE Files] を選択します。

ステップ 3　[Add] をクリックします。[Add a License File] ダイアログボックスが表示されます。

図 2-8　[Add a License File] ダイアログボックス

ステップ 4　[MSE Name] ドロップダウン リストから該当する MSE 名を選択します。

（注）　選択されているモビリティ サービス エンジンの UDI が、PAK 登録時に入力したものと一致していることを確認します。

ステップ 5　[Choose File] をクリックし、ライセンス ファイルを参照して選択します。

ステップ 6　[Upload] をクリックします。新たに追加されたライセンスが MSE ライセンス ファイル リストに表示されます。

タグ PAK の登録

AeroScout Web サイトでタグを登録するには、次の手順に従います。

ステップ 1　ブラウザを開いて、次の URL を入力します。

http://www.aeroscout.com/support

ステップ 2　アカウントがある場合はログインします。または [Create New Account] をクリックしてログイン、ユーザ名、およびパスワードを作成します。

新しいアカウントを作成すると、ユーザ名とパスワードを記載した通知電子メールを受信します。

ステップ 3　ログイン後、[Home] タブの [Register Products Purchased from Cisco] をクリックします。

製品を登録するには、PAK 番号、MSE ID（MSE シリアル番号（S/N））、およびインストール タイプの情報が必要です。

AeroScout から登録を確認する電子メール メッセージを受信します。

PAK 番号は、2 営業日以内に電子メールで確認されます。PAK 番号が無効な場合、有効な PAK 番号を使用して再度登録する必要があります。

タグ ライセンスのインストール

PAK を登録すると、ライセンス キーおよび Context-Aware Service ソフトウェアと『*AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide*』をダウンロードする方法を記載した電子メールを受信します。

タグ ライセンスのインストールの詳細については、次の URL で『*AeroScout Context-Aware for Tags, for Cisco Mobility Services Engine Users Guide*』を参照してください。

http://support.aeroscout.com

CHAPTER 3

モビリティ サービス エンジンの同期

この章では、Cisco ワイヤレス LAN コントローラと NCS をモビリティ サービス エンジンと同期する方法について説明します。

この章は、次の内容で構成されています。

NCS とモビリティ サービス エンジンの同期について

ここでは、NCS とモビリティ サービス エンジンを手動および自動的に同期する方法を説明します。

NCS にモビリティ サービス エンジンを追加したら、ネットワーク設計（キャンパス、ビルディング、フロア、および屋外マップ）、コントローラ（名前と IP アドレス）、特定の Catalyst 3000 シリーズおよび 4000 シリーズ スイッチ、およびイベント グループをモビリティ サービス エンジンと同期できます。

- ネットワーク設計：施設全体でのアクセス ポイントの物理的配置の論理マッピング。1 つのキャンパス、そのキャンパスを構成するビルディング、および各ビルディングのフロアという階層構造が、1 つのネットワーク設計を構成します。
- コントローラ：モビリティ サービス エンジンに関連付けられている選択されたコントローラ。モビリティ サービス エンジンと定期的にロケーション情報を交換します。定期的な同期により、正確なロケーション情報を維持できます。
- スイッチ：ネットワーク上の有線クライアントへのインターフェイスを提供する有線 Catalyst スイッチ。定期的な同期によって、ネットワーク上の有線クライアントのロケーションが正確に追跡されます。
  - モビリティ サービス エンジンは、Catalyst スタッカブル スイッチ（3750、3750-E、3560、2960、IE-3000 スイッチ）、スイッチ ブレード（3110、3120、3130、3040、3030、3020）、およびスイッチ ポートと同期できます。
  - モビリティ サービス エンジンは、Catalyst 4000 シリーズ スイッチ WS-C4948、WS-C4948-10GE、ME-4924-10GE、WS-4928-10GE、WS-C4900M、WS-X4515、WS-X4516、WS-X4013+、WS-X4013+TS、WS-X4516-10GE、WS-X4013+10GE、WS-X45-SUP6-E、および WS-X45-SUP6-LE とも同期できます。

- イベント グループ：イベントを生成するトリガーを定義する事前定義イベントのグループ。定期的な同期により、最新の定義イベントが追跡されます。イベント グループはサードパーティ アプリケーションでも作成できます。サードパーティ アプリケーションにより作成されたイベント グループの詳細については、「データベースの自動同期および Out-of-Sync アラートの設定」（P.3-5）を参照してください。
- サードパーティ要素：要素を MSE と同期する場合、サードパーティ アプリケーションにより MSE にイベント グループが作成されていることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。
- サービス アドバタイズメント：MSAP はモバイル デバイスにサービス アドバタイズメントを提供します。これにより、MSE と同期されたサービス アドバタイズメントが示されます。

モビリティ サービス エンジンの同期の前提条件

- 同期を実行する前に、コントローラ、NCS、およびモビリティ サービス エンジン間のソフトウェアの互換性を確認してください。http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html で、モビリティ サービス エンジンの最新リリース ノートを参照してください。
- モビリティ サービス エンジン、NCS、およびコントローラ間の通信は、協定世界時（UTC）で実行されます。各システムで NTP を設定すると、デバイスに UTC 時刻が提供されます。モビリティ サービス エンジンとその関連コントローラは、同一 NTP サーバと同一 NCS サーバにマップする必要があります。NTP サーバは、コントローラ、NCS、およびモビリティ サービス エンジン間で時刻を自動的に同期する必要があります。ただし、MSE のタイムゾーンは引き続き UTC に設定する必要があります。これは、wIPS アラームには MSE 時刻を UTC に設定する必要があるからです。

サードパーティ要素の操作

要素を MSE と同期する場合、MSE にサードパーティ アプリケーションによって作成されたイベント グループがあることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。

要素の削除またはサード パーティ要素としてのマーキング

要素を削除またはサード パーティ要素としてマークするには、次の手順に従います。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

[Network Designs] ページが表示されます。

ステップ 2　[Network Designs] ページで、左側のサイドバーのメニューから [Third Party Elements] を選択します。

[Third Party Elements] ページが表示されます。

ステップ 3　1 つ以上の要素を選択します。

ステップ 4　次のいずれかのボタンをクリックします。

- [Delete Event Groups]：選択されているイベント グループを削除します。

- [Mark as 3rd Party Event Group(s)]:選択されているイベント グループをサードパーティ イベント グループとしてマークします。

コントローラとモビリティ サービス エンジンの同期

ここでは、コントローラを同期し、MSE を任意のワイヤレス コントローラに割り当て、ネットワーク設計、コントローラ、有線スイッチ、またはイベント グループをモビリティ サービス エンジンから割り当て解除する方法について説明します。

コントローラ、Catalyst スイッチ、またはイベント グループの同期

ネットワーク設計、コントローラ、Catalyst スイッチ、またはイベント グループをモビリティ サービス エンジンと同期するには、次の手順に従います。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

左側のサイドバーのメニューには、[Network Designs]、[Controllers]、[Event Groups]、[Wired Switches]、[Third Party Elements]、および [Service Advertisements] のオプションがあります。

ステップ 2　左側のサイドバーのメニューから、該当するメニュー オプションを選択します。

ステップ 3　モビリティ サービス エンジンにネットワーク設計を割り当てるには、[Synchronize Services] ページの左側のサイドバーのメニューから、[Network Designs] を選択します。

[Network Designs] ページが表示されます。

ステップ 4　対応する [Name] チェックボックスをオンにして、モビリティ サービス エンジンと同期するすべてのマップを選択します。

（注）　リリース 6.0 では、モビリティ サービス エンジンに割り当てることができる最も詳細なレベルはキャンパス レベルです。リリース 7.0 以降では、このオプションはフロア レベルまで拡大されました。たとえば、floor1 を MSE 1 に、floor2 を MSE 2 に、floor3 を MSE 3 に割り当てることを選択できます。

ステップ 5　[Change MSE Assignment] をクリックします。

ステップ 6　マップと同期するモビリティ サービス エンジンを選択します。

ステップ 7　[MSE Assignment] ダイアログボックスで次のいずれかをクリックします。

- [Save] : モビリティ サービス エンジン割り当て を保存します。次のメッセージが [Network Designs] ページの [Messages] 列に黄色の矢印アイコンとともに表示されます。

  「To be assigned - Please synchronize.」

- [Cancel] : モビリティ サービス エンジン割り当ての変更内容を取り消し、[Network Designs] ページに戻ります。

また、[Reset] をクリックすると、モビリティ サービス エンジンの割り当てが取り消されます。

（注）　ネットワーク設計には、キャンパス内のフロアや、複数のビルディングが含まれている大規模キャンパス（各ビルディングが異なるモビリティ サービス エンジンによりモニタされる）などがあります。このため、単一ネットワーク設計を複数のモビリティ サービス エンジンに割り当てる必要がある場合があります。

（注）　ネットワーク設計割り当てでは、同期対象のコントローラが自動的に選択されます。

ステップ 8　[Synchronize] をクリックし、モビリティ サービス エンジン データベースを更新します。

項目を同期すると、同期済みエントリの [Sync. Status] 列に緑色の 2 つの矢印のアイコンが表示されます。

有線スイッチまたはイベント グループをモビリティ サービス エンジンに割り当てるときにも同じ手順を使用できます。モビリティ サービス エンジンへのコントローラの割り当ての詳細については、「コントローラとモビリティ サービス エンジンの同期」（P.3-3）を参照してください。

コントローラへの MSE の割り当て

サービス単位（CAS または wIPS）でモビリティ サービス エンジンを任意のワイヤレス コントローラに割り当てるには、次の手順に従います。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

ステップ 2　[Network Designs] ページで、左側のサイドバーのメニューから [Controller] を選択します。

ステップ 3　対応する [Name] チェックボックスをオンにして、モビリティ サービス エンジンに割り当てるコントローラを選択します。

ステップ 4　[Change MSE Assignment] をクリックします。

ステップ 5　コントローラと同期する必要があるモビリティ サービス エンジンを選択します。

ステップ 6　[Choose MSEs] ダイアログボックスで次のいずれかをクリックします。

- [Save]：モビリティ サービス エンジン割り当て を保存します。次のメッセージが [Controllers] ページの [Messages] 列に黄色の矢印アイコンとともに表示されます。

  「To be assigned - Please synchronize.」

- [Cancel]：モビリティ サービス エンジン割り当ての変更内容を取り消し、[Controllers] ページに戻ります。

また、[Reset] をクリックすると、モビリティ サービス エンジンの割り当てが取り消されます。

ステップ 7　[Synchronize] をクリックし、同期プロセスを実行します。

ステップ 8　モビリティ サービス エンジンが、選択されているサービスの各コントローラだけと通信していることを確認します。これは、ステータス ページの [NMSP status] リンクをクリックして確認できます。

（注）　コントローラの同期後、関連付けられているコントローラでタイムゾーンが設定されていることを確認します。

（注）　モビリティ サービス エンジンと同期するコントローラの名前は固有でなければなりません。同じ名前のコントローラが 2 つある場合は 1 つのコントローラだけが同期されます。

Catalyst スイッチまたはイベント グループをモビリティ サービス エンジンに割り当てるときにも同じ手順を使用できます。

（注）　スイッチは、1 つのモビリティ サービス エンジンとだけ同期できます。ただし、モビリティ サービス エンジンには複数のスイッチを接続できます。

ネットワーク設計、コントローラ、有線スイッチ、またはイベント グループの MSE からの割り当て解除

モビリティ サービス エンジンからネットワーク設計、コントローラ、有線スイッチ、またはイベント グループの割り当てを解除するには、次の手順に従います。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、該当するメニュー オプションを選択します。

ステップ 3　[Name] チェックボックスをオンにして 1 つ以上の要素を選択し、[Change MSE Assignment] をクリックします。[Choose MSEs] ダイアログボックスが表示されます。

ステップ 4　モビリティ サービス エンジンに要素を関連付けない場合は、[CAS] または [wIPS] のいずれかのチェックボックスをオンにしてモビリティ サービス エンジンの選択を解除します。

ステップ 5　[Save] をクリックして割り当ての変更を保存します。

ステップ 6　[Synchronize] をクリックします。

[Sync Status] 列がブランクになります。

データベースの自動同期および Out-of-Sync アラートの設定

NCS とモビリティ サービス エンジン データベースの手動同期はただちに実行されます。ただし、将来のデプロイメントの変更（マップやアクセス ポイントの位置の変更など）が原因で、再同期までは、ロケーションの計算やアセットの追跡が正しく行われないことがあります。

同期していない状態が発生しないようにするため、NCS を使用して同期を実行します。このポリシーにより、NCS とモビリティ サービス エンジン データベース間の同期が定期的に実行され、関連アラームがすべてクリアされます。

1 つ以上の同期コンポーネントに対する変更は、モビリティ サービス エンジンと自動的に同期されます。たとえば、アクセス ポイントが設置されているフロアを特定のモビリティ サービス エンジンと同期し、その後 1 つのアクセス ポイントが同じフロアの新しいロケーション、または別のフロア（モビリティ サービス エンジンと同期されるフロア）に移動すると、アクセス ポイントの変更後のロケーションが自動的に伝達されます。

NCS と MSE が同期されるようにするため、バックグラウンドでスマート同期が実行されます。

この項では、次のトピックを扱います。

データベースの自動同期の設定

スマート同期を設定するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　[Mobility Service Synchronization] チェックボックスをオンにします。

[Mobility Services Synchronization] ページが表示されます。

ステップ 3　モビリティ サービス エンジンが Out-of-Sync アラートを送信するように設定するには、[Out of Sync Alerts] の [Enabled] チェックボックスをオンにします。

ステップ 4　スマート同期を有効にするには、[Smart Synchronization] の [Enabled] チェックボックスをオンにします。

（注）　スマート同期は、モビリティ サービス エンジンに割り当てられていない要素（ネットワーク設計、コントローラ、またはイベント グループ）には適用されません。ただし、これらの未割り当て要素に関する out-of-sync アラームは生成されます。スマート同期をこれらの要素に適用するには、これらの要素をモビリティ サービス エンジンに手動で割り当てる必要があります。

（注）　NCS にモビリティ サービス エンジンが追加されると、NCS のデータは常に、モビリティ サービス エンジンと同期するプライマリ コピーとして扱われます。モビリティ サービス エンジンに含まれているが、NCS には含まれていない同期対象のネットワーク設計、コントローラ、イベント グループ、および有線スイッチはすべて、モビリティ サービス エンジンから自動的に削除されます。

ステップ 5　スマート同期の実行間隔を分数単位で入力します。

デフォルトでは、スマート同期は有効になっています。

ステップ 6　[Submit] をクリックします。

スマート コントローラの割り当てと選択のシナリオについては、「スマート コントローラの割り当てと選択のシナリオ」（P.3-7）を参照してください。

スマート コントローラの割り当てと選択のシナリオ

シナリオ 1

[Synchronize Services] ページの [Network Designs] メニューで、コントローラからのアクセス ポイントが 1 つ以上存在するフロアをモビリティ サービス エンジンと同期することを選択した場合、アクセス ポイントに接続しているコントローラが、CAS サービスのモビリティ サービス エンジンへの割り当て対象として自動的に選択されます。

シナリオ 2

コントローラからの 1 つ以上のアクセス ポイントが、モビリティ サービス エンジンと同期されるフロアに配置されている場合、アクセス ポイントに接続しているコントローラは、CAS サービスの同じモビリティ サービス エンジンに自動的に割り当てられます。

シナリオ 3

アクセス ポイントがフロアに追加され、モビリティ サービス エンジンに割り当てられます。このアクセス ポイントをコントローラ A からコントローラ B に移動すると、コントローラ B がモビリティ サービス エンジンと自動的に同期されます。

シナリオ 4

MSE と同期するフロアに配置されているすべてのアクセス ポイントが削除されると、そのコントローラは自動的にモビリティ サービス エンジン割り当てから削除されるか、または同期されなくなります。

Out-of-Sync アラーム

Out-of-Sync アラームは、重大度が Minor（黄色）のアラームであり、次の条件に対して出されます。

- NCS で要素が変更される（自動同期ポリシーによりこれらの要素がプッシュされます）
- コントローラ以外の要素がモビリティ サービス エンジン データベースに存在するが、NCS に存在しない
- 要素がモビリティ サービス エンジンに割り当てられていない（自動同期ポリシーは適用されません）

Out-of-Sync アラームは、次の条件が発生するとクリアされます。

- モビリティ サービス エンジンが削除される

（注） モビリティ サービス エンジンを削除すると、そのシステムの Out-of-Sync アラームも削除されます。また、使用可能な最後のモビリティ サービス エンジンを削除すると、「どのサーバにも割り当てられていない要素」のイベントが削除されます。

- 要素が手動または自動で同期される
- ユーザがアラームを手動でクリアする（ただしスケジュールされているタスクが次回実行されるときに、アラームが再び表示される可能性があります）

モビリティ サービス エンジンの同期ステータスの表示

NCS でサービスの同期機能を使用して、ネットワーク設計、コントローラ、スイッチ、およびイベント グループとモビリティ サービス エンジンとの同期のステータスを表示できます。

この項では、次のトピックを扱います。

モビリティ サービス エンジンの同期ステータスの表示

同期ステータスを表示するには、次の手順に従います。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Network Designs]、[Controllers]、[Event Groups]、[Wired Switches]、[Third Party Elements]、または [Service Advertisements] を選択します。

各要素の [Sync. Status] 列に、同期ステータスが表示されます。緑色の 2 つの矢印のアイコンは、対応する要素が指定サーバ（モビリティ サービス エンジンなど）と同期されていることを示します。灰色の 2 つの矢印と赤い円のアイコンは、対応する項目が指定のサーバと同期していないことを示します。

[Message] 列には、要素が同期していない場合の障害の原因が表示されます。

[Monitor] > [Site Maps] > [System Campus] > *ビルディング* > *フロア*を選択して、同期ステータスを表示することもできます。

この*ビルディング*はキャンパス内のビルディング、*フロア*はキャンパス ビルディング内の特定のフロアです。

左側のサイドバーのメニューの [MSE Assignment] オプションに、フロアが現在割り当てられているモビリティ サービス エンジンが表示されます。このページからモビリティ サービス エンジン割り当てを変更することもできます。

同期履歴の表示

モビリティ サービス エンジンの過去 30 日間の同期履歴を表示できます。アラームが自動的にクリアされるため、これは特に自動同期が有効な場合に便利です。同期履歴には、クリアされたアラームの要約が表示されます。

同期履歴を表示するには、[Services] > [Synchronization History] の順に選択します。[Synchronization History] ページが表示されます。

表 3-1、パート 1 に、[Synchronization History] ページに表示される表の列見出しを示します。

表 3-1、パート 1　[Synchronization History] ページ

テキスト ボックス	説明
Timestamp	同期が実行された日時。
Server	モビリティ サービス エンジン サーバ。
Element Name	同期された要素の名前。
Type	同期された要素のタイプ。
Sync Operation	実行された同期動作。 [Update]、[Add]、または [Delete] です。

表 3-1、パート 1　[Synchronization History] ページ （続き）

テキスト ボックス	説明
Generated By	同期の方法。 [Manual] または [Automatic] です。
Status	同期のステータス。[Success] または [Failed] のいずれかです。
Message	同期に関するその他のメッセージ。

エントリをソートするには、列見出しをクリックします。

CHAPTER 4

ハイ アベイラビリティの設定

この章では、MSE 上でハイ アベイラビリティを設定する方法について説明します。モビリティ サービス エンジンは、複数のモビリティ アプリケーションをホストするプラットフォームです。アクティブな各 MSE は別の非アクティブ インスタンスによりバックアップされます。アクティブな MSE はプライマリ MSE、非アクティブな MSE はセカンダリ MSE と呼ばれます。

ハイ アベイラビリティ システムの主要なコンポーネントは、ヘルス モニタです。ヘルス モニタは、ハイ アベイラビリティ セットアップを設定、管理、モニタします。プライマリ MSE とセカンダリ MSE の間でハートビートが維持されます。ヘルス モニタは、データベースのセットアップ、ファイルのレプリケーション、アプリケーションのモニタリングを行います。プライマリ MSE で障害が発生し、セカンダリ MSE に切り替わると、プライマリ MSE の仮想アドレスが透過的に切り替わります。

この章は、次の内容で構成されています。

ハイ アベイラビリティ アーキテクチャの概要

ここでは、ハイ アベイラビリティ アーキテクチャの概要について説明します。

- アクティブな各プライマリ MSE は別の非アクティブ インスタンスによりバックアップされます。セカンダリ MSE の目的は、プライマリ MSE のアベイラビリティと状態をモニタすることです。セカンダリ MSE は、フェールオーバー手順の開始後にアクティブになります。
- フェールオーバー手順は手動または自動です。
- 1 つのセカンダリ MSE では 2 つのプライマリ MSE をサポートできます。
- 登録されているプライマリ MSE ごとに 1 つのソフトウェアおよびデータベース インスタンスが存在します。

組み合わせ表

表 4-1 に、サーバ タイプの組み合わせに関する情報を示します。

表 4-1　組み合わせ表

	セカンダリ サーバ タイプ							
プライマリ サーバ タイプ		3310	3350	3355	VA-2	VA-3	VA-4	VA-5
	3310	Y	Y	Y	N	N	N	N
	3350	N	Y	Y	N	N	N	N
	3355	N	Y	Y	N	N	N	N
	VA-2	N	N	N	Y	Y	Y	Y
	VA-3	N	N	N	N	Y	Y	Y
	VA-4	N	N	N	N	N	Y	Y
	VA-5	N	N	N	N	N	N	Y

ハイ アベイラビリティのガイドラインと制約事項

- NCS からヘルス モニタの IP と仮想 IP の両方にアクセスできる必要があります。
- ヘルス モニタ IP と仮想 IP は常に異なる IP でなければなりません。ヘルス モニタと仮想インターフェイスは、同じインターフェイス上にあっても別のインターフェイス上にあってもかまいません。
- 手動フェールオーバーと自動フェールオーバーのいずれかを使用できます。フェールオーバーは、一時的なものであると見なす必要があります。故障した MSE をできるだけ早く復旧して、フェールバックを再開する必要があります。故障した MSE の復旧に時間がかかるほど、セカンダリ MSE を共有する他の MSE をフェールオーバー サポートなしで稼働する時間が長くなります。
- 手動フェールバックと自動フェールバックのいずれかを使用できます。
- プライマリ MSE とセカンダリ MSE は、同じソフトウェア バージョンを実行する必要があります。
- WAN 上のハイ アベイラビリティはサポートされません。
- LAN 上のハイ アベイラビリティは、プライマリ MSE とセカンダリ MSE の両方が同じサブネット内にある場合に限りサポートされます。
- プライマリとセカンダリの MSE が通信するポートを開ける（ネットワーク ファイアウォール、アプリケーション ファイアウェイ、ゲートウェイなどでブロックしない）必要があります。

ハイ アベイラビリティのフェールオーバー シナリオ

プライマリ MSE で障害が検出されると、次のイベントが発生します。

（注）　1 つのセカンダリ MSE が複数のプライマリ MSE をバックアップできます。

- セカンダリ MSE のヘルス モニタにより、プライマリ MSE が機能していないこと（ハードウェア障害、ネットワーク障害など）が確認されます。

- 自動フェールオーバーが有効に設定されている場合、セカンダリ MSE がただちに起動し、プライマリ MSE の該当するデータベースを使用します。自動フェールオーバーが無効にされている場合は、フェールオーバーを手動で開始するかどうかを確認する電子メールが管理者に送信されます。
- 手動フェールオーバーが設定されていると、電子メールが MSE アラーム用に設定されている場合にだけ電子メールが送信されます。手動フェールオーバーが設定されていて、呼び出されない場合、フェールバックの必要はありません。
- フェールバックが呼び出され、プライマリ MSE がすべての操作を実行するようになります。
- フェールオーバー操作の結果はヘルス モニタ UI でイベントとして示され、クリティカル アラームが管理者に送信されます。

フェールバック

セカンダリ MSE がすでにプライマリ MSE をフェールオーバーしている場合、プライマリ MSE が通常の状態に戻ると、フェールバックを呼び出すことができます。

フェールバックが発生するのは、セカンダリ MSE がプライマリ インスタンスに対して次のいずれかの状態である場合だけです。

- セカンダリ MSE が実際にプライマリ MSE をフェールオーバーしている。
- 手動でのフェールオーバーが設定されているが、管理者が呼び出さなかった。
- プライマリ MSE で障害が発生したが、エラーが検出されたか、またはセカンダリ MSE が別のプライマリ MSE をフェールオーバーしていることが原因で、セカンダリ MSE が引き継ぐことができない。
- フェールバックは、障害が発生したプライマリ MSE を管理者が起動する場合にだけ行われます。

HA ライセンス

MSE HA システムをセットアップする場合、別途ライセンスは必要ありません。仮想アプライアンス セカンダリにはアクティベーション ライセンスは必要ありません。

MSE でのハイ アベイラビリティの設定

MSE でハイ アベイラビリティを設定するには、次の 2 つの操作を行う必要があります。

- MSE ソフトウェアのインストール中に、コマンドライン クライアントを使用して特定の設定を行う必要があります。
- NCS UI からプライマリ MSE とセカンダリ MSE を組み合わせます。

（注） ハイ アベイラビリティ サポートを使用しない場合、および古いリリースからのアップグレードを実行している場合は、引き続き MSE の古い IP アドレスを使用してください。ハイ アベイラビリティをセットアップするには、ヘルス モニタの IP アドレスを設定する必要があります。したがって、ヘルス モニタが仮想 IP アドレスになります。

（注） デフォルトでは、すべての MSE がプライマリとして設定されます。

プライマリ MSE でハイ アベイラビリティを設定するには、次の手順に従います。

ステップ 1　プライマリとセカンダリの間のネットワーク接続が機能しており、すべての必要なポートが開いていることを確認します。

ステップ 2　正しいバージョンの MSE をプライマリ MSE 上にインストールします。

ステップ 3　他のプライマリ MSE 上およびセカンダリ MSE 上でロードされているリリース バージョンと同じ MSE リリース バージョンが、新しいプライマリ MSE 上にもロードされていることを確認します。

ステップ 4　プライマリ MSE で次のコマンドを入力します。

```
/opt/mse/setup/setup.sh
----------------------------------------------------------------
Welcome to the appliance setup.
Please enter the requested information.  At any prompt,
enter ^ to go back to the previous prompt. You may exit at
any time by typing <Ctrl+C>.
You will be prompted to choose whether you wish to configure a
parameter, skip it, or reset it to its initial default value.
Skipping a parameter will leave it unchanged from its current
value.
Changes made will only be applied to the system once all the
information is entered and verified.
----------------------------------------------------------------
```

ステップ 5　ホスト名を設定します。

```
Current hostname=[mse]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

ホスト名は、ネットワーク上のデバイスを識別できる一意の名前にしてください。ホスト名は、文字で開始し、文字または数字で終了し、文字、数字、およびダッシュだけを含みます。

ステップ 6　ドメイン名を設定します。

デバイスが属するネットワーク ドメインのドメイン名を入力します。ドメイン名は、文字で開始し、*.com* などの有効なドメイン名サフィックスで終了します。ドメイン名には、文字、数字、ダッシュ、ピリオドを使用できます。

```
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 7　HA ロールを設定します。

```
Current role=[Primary]
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary):
Select role [1 for Primary, 2 for Secondary] [1]: 1
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and NCS to communicate among
themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:eth0
----------------------------------------------------------------------
Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
----------------------------------------------------------------------
```

ステップ 8　イーサネット インターフェイス パラメータを設定します。

```
Select direct connect interface [eth0/eth1/none] [none]: eth0
Enter a Virtual IP address for first this primary MSE server:
Enter Virtual IP address [172.31.255.255]:
Enter the network mask for IP address 172.31.255.255.
Enter network mask [255.255.255.0]:
Current IP address=[172.31.255.255]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[172.31.255.256
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 9　「eth1」インターフェイス パラメータの入力を求められた場合、Skip と入力して次の手順に進みます。2 つめの NIC は操作に必要ではありません。

```
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

セカンダリ MSE を設定するには、ステップ 10 ～ステップ 13 に従います。

ステップ 10　セカンダリ MSE のホスト名を設定します。

```
Current hostname=[]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 11　ドメイン名を設定します。

```
Current domain=
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 12　HA ロールを設定します。

```
Current role=[Primary]
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary)
Select role [1 for Primary, 2 for Secondary] [1]: 2
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and NCS to communicate among
themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:[eth0/eth1]
----------------------------------------------------------------------
Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
----------------------------------------------------------------------
```

ステップ 13　イーサネット インターフェイス パラメータを設定します。

```
Select direct connect interface [eth0/eth1/none] [none]: eth1
Enter a Virtual IP address for first this primary MSE server
Enter Virtual IP address [172.19.35.61]:
Enter the network mask for IP address 172.19.35.61:
Enter network mask [255.255.254.0]:
Current IP address=[172.19.35.127]
Current eth0 netmask=[255.255.254.0]
Current gateway address=[172.19.34.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 14　プライマリ MSE とセカンダリ MSE の両方を設定したら、NCS UI を使用してプライマリ MSE とセカンダリ MSE の組み合わせを設定する必要があります。

ステップ 15　プライマリ MSE が適切に追加されたら、[Services] > [High Availability] の順に選択するか、または [Services] > [Mobility Services Engine] ページを選択してこのページでプライマリ MSE デバイスをクリックし、左側のサイドバーのメニューから [HA Configuration] > [Service High Availability] の順に選択します。

[HA Configuration] ページが表示されます。

ステップ 16　プライマリ MSE とペアにするセカンダリ デバイスの名前を入力します。

ステップ 17　セカンダリ IP アドレス（セカンダリ MSE のヘルス モニタ IP アドレス）を入力します。

ステップ 18　セカンダリのパスワードを入力します。これは、MSE 上で設定されている NCS 通信パスワードです。

ステップ 19　フェールオーバー タイプを指定します。[Failover Type] ドロップダウン リストから [Manual] または [Automatic] を選択できます。10 秒後にシステムがフェールオーバーします。セカンダリ サーバは、プライマリ サーバからの次のハートビートを最大 10 秒間待機します。10 秒以内にハートビートを受信しないと、失敗が宣言されます。

ステップ 20　[Failback Type] ドロップダウン リストから [Manual] または [Automatic] を選択して、フェールバック タイプを指定します。

ステップ 21　[Long Failover Wait] に秒単位で値を指定します。

10 秒後にシステムがフェールオーバーします。最大フェールオーバー待機時間は 2 秒です。

ステップ 22　[Save] をクリックします。

ペアリングと同期が自動的に行われます。

ステップ 23　プライマリ MSE からハートビートを受信しているかどうかを確認するには、[Services] > [Mobility Services Engine] の順に選択するか、[Device Name] をクリックして設定されているパラメータを表示します。

ステップ 24　左側のサイドバーのメニューから [HA Configuration] > [Service High Availability] の順に選択します。

プライマリ MSE からハートビートを受信しているかどうかを確認します。

ハイ アベイラビリティについて設定されているパラメータの表示

ハイ アベイラビリティについて設定されているパラメータを表示するには、次の手順に従います。

ステップ 1　[Services] > [High Availability] の順に選択します。

ステップ 2　[Device Name] をクリックして、設定されているフィールドを表示します。

[HA Configuration] ページが表示されます。

ステップ 3　左側のサイドバー メニューから [Services High Availability] > [HA Configuration] の順に選択します。[HA Configuration] ページには次の情報が表示されます。

- Primary Health Monitor IP
- Secondary Device Name
- Secondary IP Address
- Secondary Password

- Failover Type
- Failback Type
- Long Failover Wait

ハイ アベイラビリティ ステータスの表示

ハイ アベイラビリティ ステータスを表示するには、次の手順に従います。

ステップ 1　[Services] > [High Availability] の順に選択します。

ステップ 2　[Device Name] をクリックして、該当するステータスを表示します。

[HA Configuration] ページが表示されます。

ステップ 3　左側のサイドバーのメニューから [Services High Availability] > [HA Status] の順に選択します。[HA Configuration] ページには次の情報が表示されます。

- Current high Availability Status
  - [Status] : プライマリ MSE インスタンスとセカンダリ MSE インスタンスが正しく同期されているかどうかを示します。
  - [Heartbeats] : プライマリ MSE からハートビートを受信しているかどうかを示します。
  - [Data Replication] : プライマリ データベースとセカンダリ データベース間でデータ レプリケーションが実行されているかどうかを示します。
  - [Mean Heartbeat Response Time] : プライマリ MSE インスタンスとセカンダリ MSE インスタンス間での平均ハートビート応答時間を示します。
- [Event Log] : MSE により生成されるすべてのイベントを表示します。最新 20 イベントを表示できます。

CHAPTER 5

MSE 配信モード

Cisco MSE は、さまざまなパフォーマンス特性を持つ物理アプライアンスにプリインストールされます。MSE は、物理アプライアンスと仮想アプライアンスの 2 つのモードで提供されます。

この章は、次の内容で構成されています。

物理アプライアンス

物理アプライアンスに MSE を配置する場合、標準の License Center UI を使用して新規ライセンスを追加できます。物理アプライアンスに MSE を配置する場合、ライセンス インストール プロセスは Cisco UDI（Unique Device Identifier）に基づきます。NCS UI で [Administration] > [License Center] を選択して、ライセンスを追加します。

物理アプライアンスの詳細については、『*Cisco Prime Network Control System Getting Started Guide, Release 1.0*』を参照してください。

（注） 仮想アプライアンス ライセンスは物理アプライアンスでは使用できません。

仮想アプライアンス

MSE は、下位レベル、ハイ エンド、および超ハイ エンドの展開をサポートするために、仮想アプライアンスとしても提供されます。仮想アプライアンスに MSE を配置する場合、ライセンスは、UDI ではなく、VUDI（Virtual Unique Device Identifier）に対して検証されます。

（注） MSE は、リリース 7.2 以降の仮想アプライアンスとして使用できます。仮想アプライアンスは、他のサービスのライセンスをインストールする前に、最初にアクティブにする必要があります。

MSE 仮想アプライアンス ソフトウェアは、Open Virtualization Archive（OVA）ファイルとして配布されます。MSE 仮想アプライアンスは、VMware 環境でサポートされる OVF を展開するための方法のいずれかを使用してインストールできます。開始する前に、MSE 仮想アプライアンスの配布アーカイブが、vSphere Client を実行しているコンピュータからアクセス可能な場所にあることを確認します。

仮想アプライアンスの場合は、アクティベーション ライセンスが必要です。アクティベーション ライセンスがない場合、MSE は評価モードで開始されます。サービス ライセンスがホスト上に存在する場合でも、アクティベーション ライセンスがインストールされていないとサービス ライセンスは拒否されます。

（注）　VMware 環境の設定の詳細については、VMware vSphere 4.0 のマニュアルを参照してください。

MSE を初めてインストールしている場合は [Services] > [Mobility Services Engine] > [Add Mobility Services Engine] ページを使用して、仮想アプライアンス ライセンスを追加および削除できます。または、[Administration] > [License Center] ページを使用してライセンスを追加または削除できます。

モビリティ サービス エンジン ウィザードを使用したライセンスの追加およびライセンスの削除については、「モビリティ サービス エンジンの NCS への追加」（P.2-4）および「NCS からのモビリティ サービス エンジンの削除」（P.2-7）を参照してください。

この項では、次のトピックを扱います。

オペレーティング システムの要件

次の OS がサポートされています。

- Red Hat Linux Enterprise Server 5.4 64 ビット オペレーティング システム インストールがサポートされます。
- Red Hat Linux バージョンでは、ローカル ストレージまたはファイバ チャネル経由の SAN のいずれかを備えた VMware ESX/ESXi バージョン 4.1 以降がサポートされます。

（注）　仮想アプライアンスで推奨される展開は、UCS と ESX/ESXi です。

クライアントの要件

MSE ユーザ インターフェイスには、Google Chrome プラグインまたは Mozilla Firefox 3.6 以降のリリースとともに Microsoft Internet Explorer 7.0 以降が必要です。

（注）　サードパーティのブラウザ拡張は有効にしないことを強く推奨します。Internet Explorer では、[Tools] > [Internet Options] を選択して、[Advanced] タブで [Enable third-party browser extensions] チェックボックスを選択解除することで、サードパーティのブラウザ拡張を無効にできます。

ブラウザを実行するクライアントには、最小で 1 GB のメモリと 2 GHz のプロセッサが必要です。クライアント デバイスでは、CPU やメモリを大量に使用するアプリケーションを実行しないでください。

サーバに MSE 仮想アプライアンスを設定するための前提条件

MSE 仮想アプライアンスを設定する前に、次の項目が完了していることを確認してください。

- コンピュータが 500 GB 以上のハード ディスク領域と拡張 RAID コントローラを搭載した高速 SAS ドライブを備えていることを確認します。
- VM ESXi 4.1 以降を使用します。
- ESXi 4.1 以降の DVD を挿入し、ドライブから起動します。ESXi をインストールします。複数のドライブがある場合、ブート ドライブとして設定されているドライブにインストールします。インストールに不適切なドライブを選択した場合は、Fedora Live CD を使用して再フォーマットし、ESXi の再インストール時に別のドライブを選択することができます。
- ESX/i のデフォルトのユーザ名およびパスワードは root および空白です。空白のまま Enter を押します（パスワードはありません）。
- IP アドレスを設定し、適切なネットワーク アダプタを選択していることを確認します（有効でアクティブなネットワーク アダプタを選択します。ホストが複数のネットワークに接続されている場合、複数を選択できます）。
- （UCS ボックスを使用している場合）CIMC の設定時に同じ IP アドレスを設定することもできます（起動中に F8 を押します）。また、デフォルトのパスワードを変更します。
- ESXi が設定されると、Windows XP/7 マシンを使用し、上記の設定済み IP アドレスとログイン クレデンシャルを使用して vSphere Client を介して ESXi ホストに接続することができます。
- ESXi でデータストアを設定するには、次の情報を参照してください。
  - http://pubs.vmware.com/vsphere-esxi-4-1-embedded/wwhelp/wwhimpl/js/html/wwhelp.htm

仮想アプライアンスのサイジング

仮想アプライアンスのサイジングについては、表 5-1 を参照してください。

表 5-1　仮想アプライアンスのサイジング

プライマリ MSE	リソース		サポートされるライセンス（個別）	
仮想アプライアンス レベル	メモリ合計	CPU	CAS ライセンス	wIPS ライセンス
レベル 1	3.5 G	1	100	20
レベル 2	6 G	2	2000	2000
レベル 3	11 G	8	18000	5000
レベル 4	20 G	16	50000	10000

物理アプライアンスでの MSE の再インストール

物理アプライアンスに MSE をインストールするには、root 権限が必要です。物理アプライアンスに MSE を再インストールするには、次の手順を実行します。

ステップ 1　提供される MSE ソフトウェア イメージ DVD を挿入します。システムがブートし、コンソールが表示されます。

ステップ 2　MSE ソフトウェア イメージを再インストールするには、オプション 1 を選択します。システムがリブートし、[configure appliance] 画面が表示されます。

ステップ 3　初期設定パラメータを入力すると、システムが再度リブートします。DVD を取り出し、手順に従って MSE サーバを起動します。

MSE 仮想アプライアンスの配置

ここでは、[Deploy OVF] ウィザードまたはコマンド ラインから vSphere Client を使用して ESXi ホストに MSE 仮想アプライアンスを展開する方法について説明します。この項では、次のトピックを扱います。

- 「VMware vSphere Client からの MSE 仮想アプライアンスの展開」（P.5-4）
- 「MSE 仮想アプライアンス VM を起動するための基本設定」（P.5-7）
- 「コマンドライン クライアントを使用した MSE 仮想アプライアンスの展開」（P.5-8）

VMware vSphere Client からの MSE 仮想アプライアンスの展開

MSE 仮想アプライアンスは、vSphere Client を使用して ESXi に展開できる OVA ファイルとして配布されます。OVA は、項目の集合を単一のアーカイブにしたものです。vSphere Client では、この項で説明されているように、[Deploy OVA] ウィザードを使用して MSE 仮想アプライアンス アプリケーションを実行する仮想マシンを作成できます。

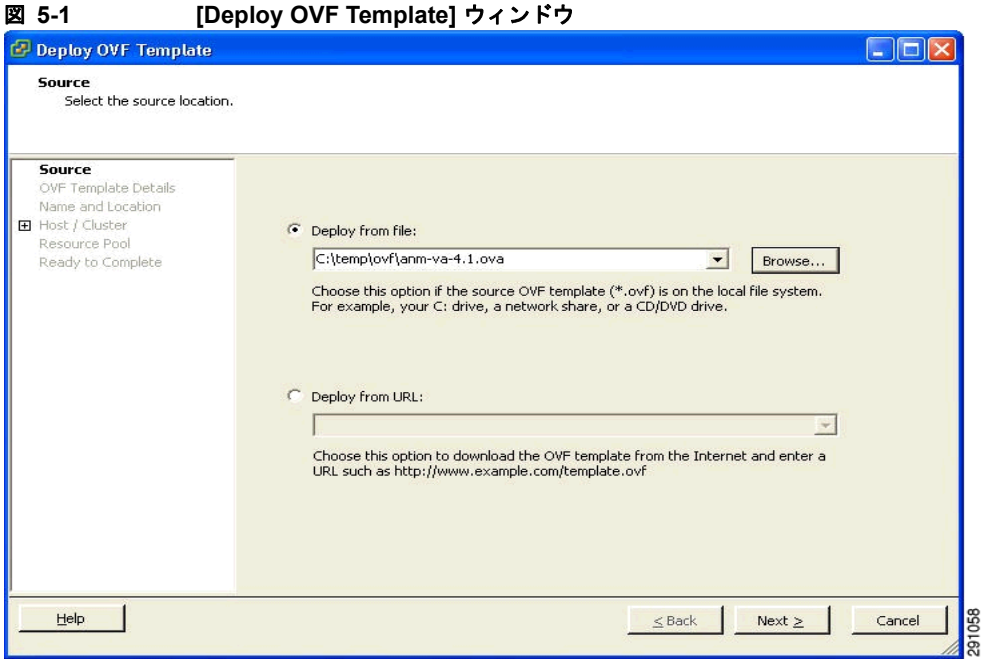
（注）　次の手順には、MSE 仮想アプライアンスの展開に関する一般的なガイドラインが記載されていますが、実行する必要がある正確な手順は、ご使用の VMware 環境と設定の特性によって異なる可能性があります。

（注）　仮想アプライアンスを展開するには、ESXi ホスト データベース上に使用可能なディスク領域が 500 GB 以上必要です。ESXi 4.1 以降には、ホスト上のデータストアのブロック サイズに 4 MB 以上を推奨します。そうでない場合、展開に失敗することがあります。ESXi 5.0 以降のデータストアにはこの制限はありません。

MSE 仮想アプライアンスを展開するには、次の手順を実行します。

ステップ 1　VMware vSphere Client のメイン メニューで、[File] > [Deploy OVF Template] を選択します。[OVF Template Source] ウィンドウが表示されます（図 5-1 を参照）。

図 5-1　[Deploy OVF Template] ウィンドウ

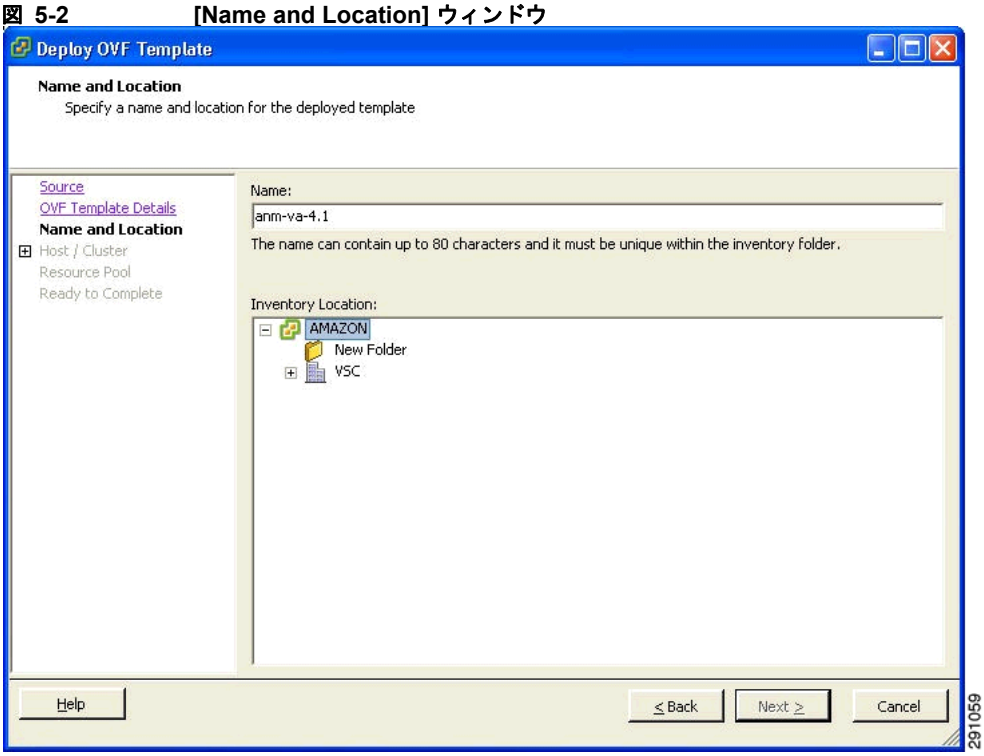


ステップ 2　[Deploy From File] オプション ボタンを選択して、ドロップダウン リストから MSE 仮想アプライアンス配布が含まれている OVA ファイルを選択します。

ステップ 3　[Next] をクリックします。[OVF Template Details] ウィンドウが表示されます。VMware ESX/ESXi が OVA 属性を読み取ります。詳細には、インストールする製品、OVA ファイルのサイズ（ダウンロード サイズ）、および仮想マシンに使用できる必要があるディスク領域の量が含まれます。

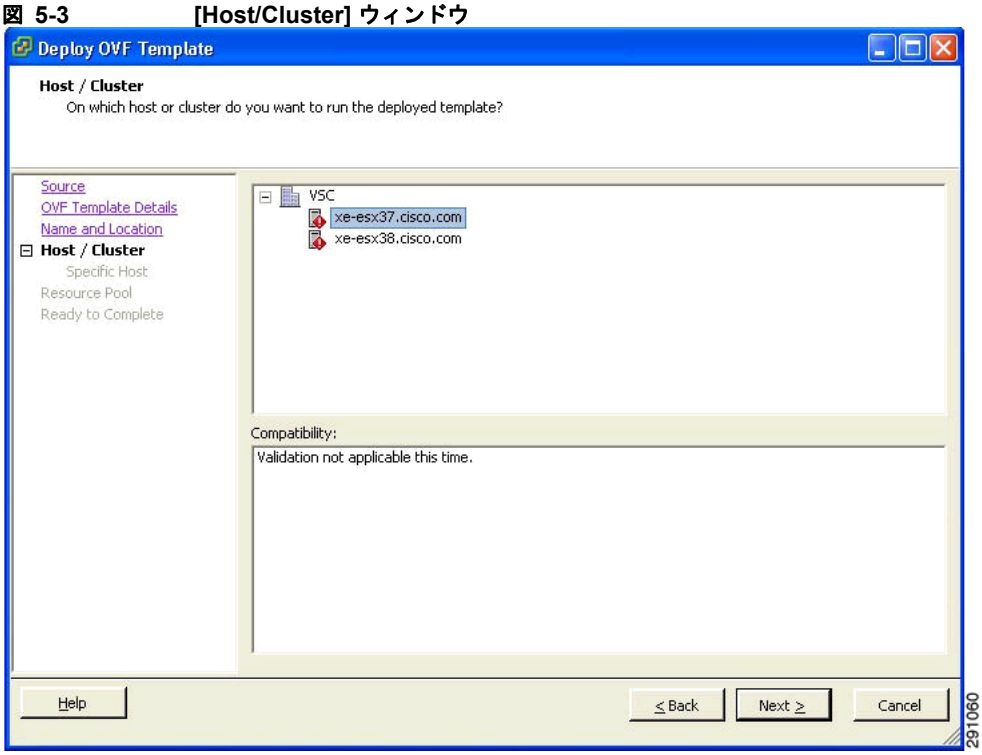
ステップ 4　OVF テンプレートの詳細を確認して、[Next] をクリックします。[Name and Location] ウィンドウが表示されます。
（図 5-2 を参照）。

図 5-2　[Name and Location] ウィンドウ



ステップ 5　[Name] テキスト ボックスで展開対象の VM のデフォルトの名前を維持するか、新しい名前を指定して、[Next] をクリックします。この名前値は、VMware インフラストラクチャで新しい仮想マシンを識別するために使用されます。この特定の VM をご使用の環境で区別する任意の名前を指定する必要があります。[Host / Cluster] ウィンドウが表示されます（図 5-3 を参照）。

図 5-3　[Host/Cluster] ウィンドウ



ステップ 6　MSE VM を展開する宛先ホストまたは HA クラスタを選択して、[Next] をクリックします。[Resource Pool] ウィンドウが表示されます。

ステップ 7　宛先ホスト環境に複数のリソース プールがある場合は、展開に使用するリソース プールを選択して、[Next] をクリックします。[Ready to Complete] ウィンドウが表示されます。

ステップ 8　展開のために表示される設定を確認して、必要に応じて [Back] をクリックして示される設定を変更します。

ステップ 9　[Finish] をクリックして、展開を完了します。インストールが完了するとメッセージで通知され、インベントリで MSE 仮想アプライアンスを確認できます。

ステップ 10　[Close] をクリックして、[Deployment Completed Successfully] ダイアログボックスを閉じます。

MSE 仮想アプライアンス VM を起動するための基本設定

新規仮想マシンへの MSE 仮想アプライアンスの展開（インストール）が完了しました。仮想マシンのノードが、VMware vSphere Client ウィンドウのリソース ツリーに表示されるようになります。OVF テンプレートを展開すると、MSE 仮想アプライアンス アプリケーションと関連するリソースがすでにインストールされた新規仮想マシンが vCenter に作成されます。展開後に、MSE 仮想アプライアンスの基本設定を行う必要があります。

MSE の設定を開始するには、次の手順を実行します。

ステップ 1　vSphere Client で、リソース ツリーの [MSE virtual appliance] ノードをクリックします。仮想マシンノードが、MSE 仮想アプライアンスを展開したホスト、クラスタ、またはリソース プールの下の Hosts and Clusters ツリーに表示されます。

ステップ 2　[Getting Started] タブで、[Basic Tasks] にある [Power on the virtual machine] というリンクをクリックします。[vSphere Client] ペインの下部にある [Recent Tasks] ウィンドウは、仮想マシンの起動に関連するタスクのステータスを示しています。仮想マシンを正常に起動した後で、タスクのステータス列に [Completed] と表示されます。

ステップ 3　キーボード入力でコンソール プロンプトをアクティブにするには、コンソール ペイン内で [Console] タブをクリックします。

ステップ 4　MSE セットアップ ウィザードを使用して設定を完了します。

コマンドライン クライアントを使用した MSE 仮想アプライアンスの展開

ここでは、コマンド ラインから MSE 仮想アプライアンスを展開する方法について説明します。vSphere Client を使用して MSE OVA 配布を展開する代わりに、コマンドライン クライアントである VMware OVF ツールを使用できます。

VMware OVF ツールを使用して OVA を展開するには、ovftool コマンドを使用します。このコマンドは、次の例に示すように、展開する OVA ファイルの名前と宛先ロケーションを引数として使用します。

```
ovftool MSE-VA-X.X.X-large.ova vi://my.vmware-host.example.com
```

この場合、展開する OVA ファイルは MSE-VA-X.X.X-large.ova で、宛先 ESX ホストは my.vmware-host.example.com です。VMware OVF ツールの詳細については、VMware vSphere 4.0 のマニュアルを参照してください。

仮想アプライアンス ライセンスの NCS への追加

次の 2 つのオプションを使用して、仮想アプライアンス ライセンスを NCS に追加できます。

- MSE を初めてインストールする場合、[Add Mobility Service Engine] ページを使用する。詳細については、「モビリティ サービス エンジンの NCS への追加」（P.2-4）を参照してください。
- [License Center] ページを使用する。詳細については、「License Center を使用したライセンス ファイルの MSE への追加」（P.5-8）を参照してください。

License Center を使用したライセンス ファイルの MSE への追加

ライセンスを追加するには、次の手順を実行します。

ステップ 1　MSE 仮想アプライアンスをインストールします。

ステップ 2　MSE を NCS に追加します。

ステップ 3　NCS UI で [Administration] > [License Center] を選択して、[License Center] ページにアクセスします。

ステップ 4　左側のサイドバーのメニューから、[Files] > [MSE Files] を選択します。

ステップ 5　[Add] をクリックして、ライセンスを追加します。

[Add A License File] メニューが表示されます。

ステップ 6　MSE を選択し、アクティベーション ライセンス ファイルを参照します。

ステップ 7　[Submit] をクリックします。

送信したら、ライセンスがアクティブになり、[License Center] ページにライセンス情報が表示されます。

License Center を使用した MSE ライセンス情報の表示

License Center では、NCS、ワイヤレス LAN コントローラ、および MSE のライセンスを管理できます。ライセンス情報を表示するには、次の手順を実行します。

ステップ 1　[Administration] > [License Center] を選択して、[License Center] ページにアクセスします。

ステップ 2　左側のサイドバーのメニューから、[Summary] > [MSE] を選択して、[MSE Summary] ページを表示します。

表 5-2 に、[MSE Summary] ページのフィールドの一覧を示します。

表 5-2　[MSE Summary] ページ

フィールド	説明
MSE Name	MSE ライセンス ファイルのリスト ページへのリンクを提供します。
Service	サービスのタイプは CAS または wIPS です。
Platform Limit	プラットフォームの制限。
Type	MSE のタイプを指定します。
Installed Limit	MSE 上でライセンス付与されたクライアント要素の合計数を表示します。
License Type	永久、評価、および拡張の 3 つの異なるタイプのライセンス。
Count	MSE 上で現在ライセンス付与されている CAS または wIPS の要素数。
Unlicensed Count	ライセンス付与されていないクライアント要素の数を表示します。
%Used	MSE 上でライセンス付与されている CAS または wIPS の要素の割合。

License Center を使用したライセンス ファイルの削除

ライセンスを削除するには、次の手順を実行します。

ステップ 1　MSE 仮想アプライアンスをインストールします。

ステップ 2　ウィザードを使用して MSE を NCS に追加します。

ステップ 3　[Administration] > [License Center] を選択して、[License Center] ページにアクセスします。

ステップ 4　左側のサイドバーのメニューから、[Files] > [MSE Files] を選択します。

ステップ 5　[MSE License File] オプション ボタンを選択して、削除する MSE ライセンス ファイルを選択し、[Remove] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。

CHAPTER 6

システム プロパティの設定および表示

この章では、モビリティ サービス エンジンでシステム プロパティを設定および表示する方法を説明します。

この章は、次の内容で構成されています。

ライセンス要件

モビリティ サービス エンジンには CAS および wIPS の評価ライセンスが付属しています。評価版は 60 日間（480 時間）有効で、各サービスに対してデバイスの制限が事前設定されています。ライセンスは使用ベースです（時間は、経過した暦日の数ではなく、使用した日数だけ減少します）。

ライセンスの購入およびインストールの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

一般プロパティの編集およびパフォーマンスの表示

一般プロパティ：Cisco NCS を使用してモビリティ サービス エンジンの一般プロパティを編集できます。一般プロパティには、連絡先名、ユーザ名、パスワード、システム上で有効なサービス、サービスの有効化または無効化、同期のためのモビリティ サービス エンジンの有効化などがあります。詳細については、「一般プロパティの編集」（P.6-2）を参照してください。

（注） モビリティ サービス エンジンの初期設定時に定義したユーザ名とパスワードを変更するには、一般プロパティを使用します。

パフォーマンス：NCS を使用して特定のモビリティ サービス エンジンの CPU およびメモリの使用率を表示できます。詳細については、「パフォーマンス情報の表示」（P.6-4）を参照してください。

この項では、次のトピックを扱います。

一般プロパティの編集

モビリティ サービス エンジンの一般プロパティを編集するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択し、[Mobility Services] ページを表示します。

ステップ 2　編集するモビリティ サービス エンジンの名前をクリックします。[General] と [Performance] の 2 つのタブが表示されます。

（注）　デフォルトで [General Properties] ページが表示されない場合、左側のサイドバーのメニューから [Systems] > [General Properties] の順に選択します。

ステップ 3　[General] タブで、必要に応じてフィールドを変更します。表 6-1 に [General Properties] ページのフィールドの一覧を示します。

表 6-1　[General] タブ

フィールド	設定オプション
Device Name	モビリティ サービス エンジンのユーザ割り当て名。
Device Type	モビリティ サービス エンジンのタイプを示します（例：Cisco 3310 Mobility Services Engine）。デバイスが仮想アプライアンスであるかどうかを示します。
Device UDI	デバイス UDI（Unique Device Identifier）ストリングは二重引用符で囲まれています（ストリングの末尾にスペースがある場合はスペースも含まれます）。
Version	製品 ID のバージョン
Start Time	サーバが起動された起動時刻を示します。
IP Address	モビリティ サービス エンジンの IP アドレスを示します。
Contact Name	モビリティ サービス エンジンの連絡先名を入力します。
Username	モビリティ サービス エンジンを管理する NCS サーバのログイン ユーザ名を入力します。これにより、初期設定時に設定されたユーザ名を含む、以前に定義されたユーザ名が置き換えられます。
Password	モビリティ サービス エンジンを管理する NCS サーバのログイン パスワードを入力します。これにより、初期設定時に設定されたパスワード名を含む、以前に定義されたパスワードが置き換えられます。
HTTP	HTTP を有効にするには、[Enable] チェックボックスをオンにします。デフォルトでは、HTTPS が有効です。 **（注）**　HTTP は、主にサードパーティ アプリケーションがモビリティ サービス エンジンと通信できるようにするために有効にします。 **（注）**　NCS は常に HTTPS を使用して通信します。

表 6-1　[General] タブ （続き）

フィールド	設定オプション
Legacy Port	HTTPS 通信をサポートするモビリティ サービスのポート番号を入力します。[Legacy HTTPS] オプションも有効にする必要があります。
Legacy HTTPS	これはモビリティ サービス エンジンには適用されません。ロケーション アプライアンスにのみ適用されます。
Delete synchronized service assignments and enable synchronization	モビリティ サービス エンジンからすべてのサービス割り当てを永久に削除するには、このチェックボックスをオンにします。このオプションを使用できるのは、モビリティ サービス エンジンを追加するときに [Delete synchronized service assignments] チェックボックスをオフにした場合だけです。
Mobility Services	モビリティ サービス エンジン上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。このサービスには Context Aware および wIPS が含まれます。 CAS を選択すると、クライアント、不正アクセス ポイント、干渉、有線クライアント、およびタグを追跡できます。 タグを追跡するには、次のいずれかのエンジンを選択します。 • Cisco Tag Engine または • Partner Tag Engine **（注）** 選択すると、サービスは [Up]（アクティブ）として表示されます。アクティブでないサービスはすべて、選択された（現行）システム上およびネットワーク上で [Down]（非アクティブ）として表示されます。 **（注）** CAS および wIPS はモビリティ サービス エンジン上で同時に稼働できます。 現在のシステムで割り当て可能なデバイスの数を確認するには、[here] リンクをクリックします。 ネットワーク上のすべてのモビリティ サービス エンジンのライセンスの詳細を表示するには、[License Center] ページで、左側のサイドバーのメニュー オプションから [MSE] を選択します。 **（注）** ライセンスの購入およびインストールの詳細については、次の URL を参照してください。 http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

（注） リリース 6.0 の MSE で使用される TCP ポートは、tcp 22（MSE SSH ポート）、tcp 80（MSE HTTP ポート）、tcp 443（MSE HTTPS ポート）、tcp 1411（AeroScout）、tcp 1999（AeroScout 内部ポート）、tcp 4096（AeroScout 通知ポート）、tcp 5900X（AeroScout）（X は 1 ～ 10）、tcp 8001（レガシー ポート）です。ロケーション API に使用されます。

（注）　リリース 6.0 の MSE で使用される UDP ポートは、udp 123（NTPD ポート、NTP 設定の後に開きます）、udp 162（AeroScout SNMP）、udp/tcp 4000X（AeroScout プロキシ、X は 1 ～ 5）、udp 12091（AeroScout デバイス）（TDOA Wi-Fi レシーバ、チョークポイント）、udp 12092（AeroScout デバイス）（TDOA Wi-Fi レシーバ、チョークポイント）、udp 32768（ロケーション内部ポート）、udp 32769（AeroScout 内部ポート）、udp 37008（AeroScout 内部ポート）です。

（注）　MSE で **enable http** コマンドを入力した場合、MSE でポート 80 が有効になります。CA が発行する証明書が MSE にインストールされている場合、MSE でポート 8880 および 8843 は閉じられます。

図 6-1　　選択したモビリティ サービス エンジンのライセンスの概要

ステップ 4　[Save] をクリックして NCS とモビリティ サービス エンジン データベースを更新します。

パフォーマンス情報の表示

パフォーマンスの詳細を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択し、[Mobility Services] ページを表示します。

ステップ 2　表示するモビリティ サービス エンジンの名前をクリックします。[General] と [Performance] の 2 つのタブが表示されます。

ステップ 3　[Performance] タブをクリックします（図 6-2 を参照）。

1 日を超える期間のパフォーマンスの数値を表示するには、y 軸上の期間（[1w] など）をクリックします。

パフォーマンスの概要をテキストで表示するには、CPU の下の 2 つ目のアイコンをクリックします。

ページを拡大するには、右下にあるアイコンをクリックします。

図 6-2　CPU およびメモリのパフォーマンス

システムのアクティブ セッションの表示

モビリティ サービス エンジンのアクティブなユーザ セッションを表示できます。

各セッションに関する次の情報が表示されます。

- セッション ID
- モビリティ サービス エンジンのアクセス元の IP アドレス
- 接続ユーザのユーザ名
- セッションが開始された日時
- モビリティ サービス エンジンが最後にアクセスされた日時
- 最終アクセス以降セッションがアイドルになっていた期間

アクティブなユーザ セッションを表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　アクティブ セッションを表示するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Active Sessions] の順に選択します。

トラップ宛先の追加および削除

モビリティ サービス エンジンにより生成される SNMP トラップを受信する NCS または Cisco Security Monitoring, Analysis, and Response System（CS-MARS）ネットワーク管理プラットフォームを指定できます。

NCS を使用してモビリティ サービス エンジンを追加すると、その NCS プラットフォームは自動的に自身をデフォルトのトラップ宛先として設定します。冗長 NCS 設定が存在する場合、プライマリ NCS に障害が発生し、バックアップ システムに切り替わらない限り、バックアップ NCS はデフォルトのトラップ宛先としてリストされません。アクティブな NCS だけがトラップ宛先としてリストされます。

この項では、次のトピックを扱います。

トラップ宛先の追加

トラップ宛先を追加するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　新しい SNMP トラップ宛先サーバを定義するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Trap Destinations] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add Trap Destination] を選択します。[Go] をクリックします。

[New Trap Destination] ページが表示されます。

表 6-2 に、[Add Trap Destination] ページのフィールドの一覧を示します。

表 6-2　[Add Trap Destination] ページのフィールド

フィールド	説明
IP Address	トラップ宛先の IP アドレス。
Port No.	トラップ宛先のポート番号。デフォルト ポート番号は、162 です。
Destination Type	このフィールドは編集できず、値 [Other] が表示されます。
SNMP Version	[SNMP Version] ドロップダウン リストから [v2c] または [v3] を選択します。
SNMP バージョンとして v3 を選択した場合にだけ表示されるフィールドを以下に示します。	
User Name	SNMP バージョン 3 のユーザ名。
Security Name	SNMP バージョン 3 のセキュリティ名。
Auth.Type	ドロップダウン リストから、次のいずれかを選択します。 • HMAC-MD5 • HMAC-SHA

表 6-2　[Add Trap Destination] ページのフィールド （続き）

フィールド	説明
Auth.Password	SNMP バージョン 3 の認証パスワード。
Privacy Type	ドロップダウン リストから、次のいずれかのオプションを選択します。 • CBC-DES • CFB-AES-128 • CFB-AES-192 • CFB-AES-256
Privacy Password	SNMP バージョン 3 のプライバシー パスワード。

（注）　自動的に作成される*デフォルト*のトラップ宛先を除き、すべてのトラップ宛先は*その他*として識別されます。

ステップ 5　[Save] をクリックします。

[Trap Destination Summary] ページが表示され、新たに定義されたトラップがリストされます。

トラップ宛先の削除

トラップ宛先を削除するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　SNMP トラップ宛先サーバを削除するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Trap Destinations] の順に選択します。

ステップ 4　削除するトラップ宛先エントリの横にあるチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから、[Add Trap Destination] を選択します。[Go] をクリックします。

ステップ 6　表示されるダイアログボックスで、[OK] をクリックして削除を実行します。

詳細パラメータの表示および設定

[NCS Advanced Parameters] ページ（図 6-3 を参照）で、モビリティ サービス エンジンの一般的なシステム レベル設定を表示し、モニタリング パラメータを設定することができます。

- 現在のシステム レベルの詳細パラメータを表示するには、「詳細パラメータ設定の表示」（P.6-8）を参照してください。

- 現在のシステム レベルの詳細パラメータを変更するには、またはシステムの再起動、システムのシャットダウン、コンフィギュレーション ファイルの消去などの詳細コマンドを開始するには、「詳細コマンドの開始」（P.6-10）を参照してください。

詳細パラメータ設定の表示

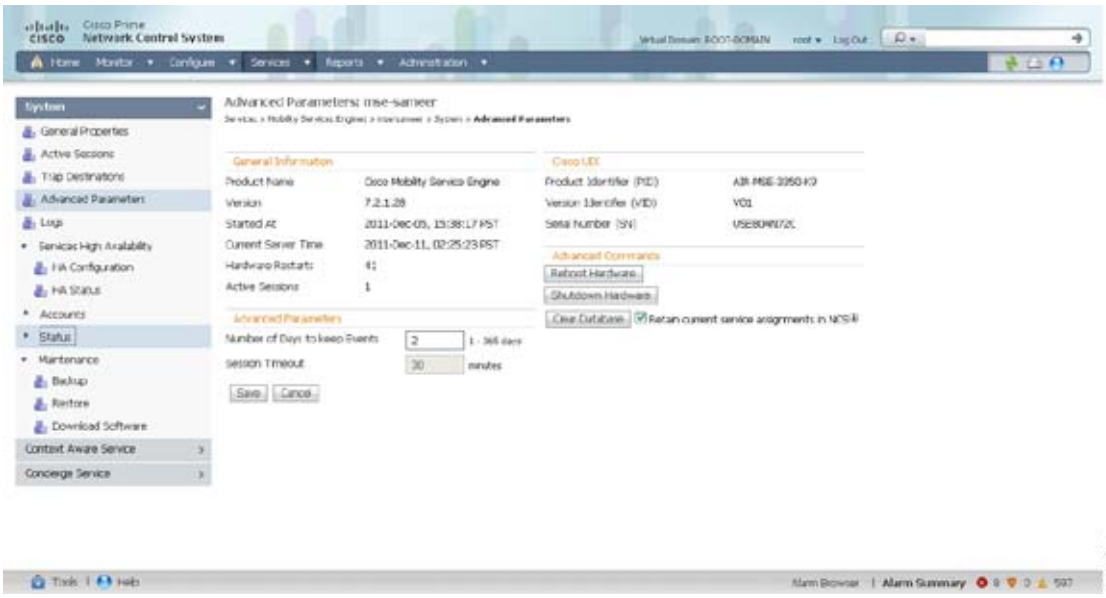
モビリティ サービス エンジンの詳細パラメータ設定を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　ステータスを表示するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Advanced Parameters] の順に選択します（図 6-3 を参照）。

図 6-3　[Advanced Parameters] ページ



詳細パラメータの開始

NCS の [Advanced Parameters] セクションでは、イベントを維持する日数およびセッション タイムアウト値を設定できます。また、システムの再起動またはシャットダウンを開始したり、システム データベースを消去したりできます。

（注）　NCS を使用して、モビリティ サービス エンジンまたはロケーション アプライアンスのトラブルシューティング パラメータを変更できます。

[Advanced Parameters] ページで、次の目的で NCS を使用できます。

- イベントを維持する期間およびセッション タイムアウトまでの期間を設定する。

詳細については、「詳細パラメータの設定」（P.6-9）を参照してください。

- システムの再起動またはシャットダウンを開始したり、システム データベースを消去する。
  詳細については、「詳細コマンドの開始」（P.6-10）を参照してください。

詳細パラメータの設定

詳細パラメータを設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Advanced Parameters] の順に選択します。

ステップ 4　必要に応じて詳細パラメータを確認または変更します。

- 全般情報
  - Product Name
  - Version
  - Started At
  - Current Server Time
  - Hardware Restarts
  - Active Sessions
- Advanced Parameters

注意　詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

  - [Number of Days to keep Events]：ログを維持する日数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。
  - [Session Timeout]：セッションがタイムアウトになるまでの分数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。現時点では、このオプションは淡色表示されます。
- Cisco UDI
  - [Product Identifier (PID)]：モビリティ サービス エンジンの製品 ID。
  - [Version Identifier (VID)]：モビリティ サービス エンジンのバージョン番号。
  - [Serial Number (SN)]：モビリティ サービス エンジンのシリアル番号。
- Advanced Commands
  - [Reboot Hardware]：モビリティ サービス ハードウェアを再起動する場合にクリックします。詳細については、「システムの再起動またはシャットダウン」（P.6-10）を参照してください。
  - [Shutdown Hardware]：モビリティ サービス ハードウェアをオフにする場合にクリックします。詳細については、「システムの再起動またはシャットダウン」（P.6-10）を参照してください。

– [Clear Database]：モビリティ サービス データベースをクリアする場合にクリックします。詳細については、「システム データベースの消去」（P.6-10）を参照してください。NCS と MSE から既存のサービス割り当てをすべて削除するには、[Retain current service assignments in NCS] チェックボックスをオフにします。[Services] > [Synchronize Services] ページでリソースを再割り当てする必要があります。デフォルトでは、このオプションが選択されています。

ステップ 5　[Save] をクリックして NCS とモビリティ サービス エンジン データベースを更新します。

詳細コマンドの開始

システムの再起動またはシャットダウンを開始したり、システム データベースを消去するには、[Advanced Parameters] ページで該当するボタンをクリックします。

この項では、次のトピックを扱います。

- 「システムの再起動またはシャットダウン」（P.6-10）
- 「システム データベースの消去」（P.6-10）

システムの再起動またはシャットダウン

モビリティ サービス エンジンを再起動またはシャットダウンするには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　再起動またはシャットダウンするモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Advanced Parameters] の順に選択します（図 6-3 を参照）。

ステップ 4　[Advanced Commands] グループ ボックスで、該当するボタン（[Reboot Hardware] または [Shutdown Hardware]）をクリックします。

確認のダイアログボックスで [OK] をクリックして、再起動またはシャットダウン プロセスを開始します。プロセスを中止するには、[Cancel] をクリックします。

システム データベースの消去

モビリティ サービス エンジン設定をクリアし、出荷時の初期状態に戻すには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　設定するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Advanced Parameters] の順に選択します。

ステップ 4　[Advanced Commands] グループ ボックスの [Retain current service assignments in NCS] チェックボックスをオフにして、NCS と MSE から既存のサービス割り当てをすべて削除します。

[Services] > [Synchronize Services] ページでリソースを再割り当てする必要があります。デフォルトでは、このオプションが選択されています。

ステップ 5　[Advanced Commands] グループ ボックスで [Clear Database] をクリックします。

ステップ 6　[OK] をクリックし、モビリティ サービス エンジン データベースをクリアします。

CHAPTER 7

ユーザとグループの管理

この章では、ユーザ、グループ、およびモビリティ サービス エンジンへのホスト アクセスを管理する方法について説明します。

この章は、次の内容で構成されています。

前提条件

Cisco NCS がモビリティ サービス エンジンにアクセスするには、フル アクセス権限が必要です。

ガイドラインと制限事項

グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフル アクセス権限を付与し、*読み取り専用*アクセス権限が付与されているグループにそのユーザを追加すると、ユーザはモビリティ サービス エンジンの設定を設定できなくなります。

ユーザ グループの管理

この項では、ユーザ グループの追加、削除、および編集の方法について説明します。

ユーザ グループを使用すると、ユーザに異なるアクセス権限を割り当てることができます。

この項では、次のトピックを扱います。

ユーザ グループの追加

モビリティ サービス エンジンにユーザ グループを追加するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　ユーザ グループを追加するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Accounts] > [Groups] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Group] を選択します。[Go] をクリックします。

ステップ 5　[Group Name] テキストボックスにグループ名を入力します。

ステップ 6　[Permission] ドロップダウン リストから権限レベル（[read]、[write]、または [full]）を選択します。

（注）　NCS がモビリティ サービス エンジンにアクセスするには、フル アクセス権限が必要です。

ステップ 7　[Save] をクリックします。

ユーザ グループの削除

モビリティ サービス エンジンからユーザ グループを削除するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　ユーザ グループを削除するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Accounts] > [Groups] の順に選択します。

ステップ 4　削除するグループのチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから、[Delete Group] を選択し、[Go] をクリックします。

ステップ 6　[OK] をクリックします。

ユーザ グループの権限の変更

注意　グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフル アクセス権限を付与し、読み取りアクセス権限のみ付与されているグループにそのユーザを追加すると、ユーザはモビリティ サービス エンジンの設定を設定できなくなります。

ユーザ グループの権限を変更するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　編集するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Accounts] > [Groups] の順に選択します。

ステップ 4　編集するグループの名前をクリックします。

ステップ 5　[Permission] ドロップダウン リストから権限レベル（[read]、[write]、または [full]）を選択します。

ステップ 6　[Save] をクリックします。

ユーザの管理

この項では、モビリティ サービス エンジンのユーザの追加、削除、および編集の方法について説明します。アクティブなユーザ セッションの表示方法についても説明します。

この項では、次のトピックを扱います。

ユーザの追加

注意　グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフル アクセス権限を付与し、読み取りアクセス権限のみ付与されているグループにそのユーザを追加すると、ユーザはモビリティ サービス エンジンの設定を設定できなくなります。

モビリティ サービス エンジンにユーザを追加するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　ユーザを追加するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Accounts] > [Users] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add User] を選択します。[Go] をクリックします。

ステップ 5　[Username] テキストボックスにユーザ名を入力します。

ステップ 6　[Password] テキストボックスにパスワードを入力します。

ステップ 7　[Confirm Password] テキスト ボックスにパスワードを再入力します。

ステップ 8　[Group Name] テキストボックスにユーザが属するグループの名前を入力します。

ステップ 9　[Permission] ドロップダウン リストから権限レベル（[read]、[write]、または [full]）を選択します。

（注）　NCS がモビリティ サービス エンジンにアクセスするには、フル アクセス権限が必要です。

ステップ 10　[Save] をクリックします。

ユーザの削除

モビリティ サービス エンジンからユーザを削除するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。
ステップ 2　ユーザを削除するモビリティ サービス エンジンの名前をクリックします。
ステップ 3　[System] > [Accounts] > [Users] の順に選択します。
ステップ 4　削除するユーザのチェックボックスをオンにします。
ステップ 5　[Select a command] ドロップダウン リストから [Delete User] を選択します。[Go] をクリックします。
ステップ 6　[OK] をクリックします。

ユーザ プロパティの変更

ユーザ プロパティを変更するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。
ステップ 2　編集するモビリティ サービス エンジンの名前をクリックします。
ステップ 3　[System] > [Accounts] > [Users] の順に選択します。
ステップ 4　編集するグループの名前をクリックします。
ステップ 5　[Password] および [Group Name] テキスト ボックスで必要な変更を行います。
ステップ 6　[Save] をクリックします。

CHAPTER 8

wIPS およびプロファイルの設定

この章では、wIPS プロファイルおよび wIPS を操作するために併せて設定する必要がある項目の設定方法について説明します。

この章は、次の内容で構成されています。

ガイドラインと制限事項

- モビリティ サービス エンジンは 1 つの NCS からのみ設定できます。
- ご使用の wIPS がコントローラ、アクセス ポイント、および MSE で構成されている場合、これら 3 つのエンティティをすべて UTC タイムゾーンに設定する必要があります。
- コントローラは 1 つの設定プロファイルに関連付けられます。そのコントローラに接続されている wIPS モード アクセス ポイントはすべて同じ wIPS 設定を共有します。

前提条件

wIPS プロファイルを設定する前に、次の手順を実行する必要があります。

1. モビリティ サービス エンジンをインストールします（まだネットワーク内で動作していない場合）。次の URL にある『*Cisco 3350 Mobility Services Engine Getting Started Guide*』または『*Cisco 3310 Mobility Services Engine Getting Started Guide*』を参照してください。

   http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html
2. モビリティ サービス エンジンを NCS に追加します（まだ追加されていない場合）。
3. wIPS モニタ モードで動作するようにアクセス ポイントを設定します。「wIPS モニタ モードのアクセス ポイントの設定」（P.8-2）を参照してください。
4. wIPS プロファイルを設定します。「wIPS プロファイルの設定」（P.8-4）を参照してください。

wIPS 設定およびプロファイル管理について

wIPS プロファイルの設定は、プロファイルの表示と変更に使用される NCS から始まるチェーン階層を進みます。実際のプロファイルは、MSE で実行するワイヤレス IPS サービス内に保存されます。

プロファイルは、モビリティ サービス エンジン上の wIPS サービスから、特定のコントローラに伝播され、次に、その各コントローラに関連付けられている wIPS モード アクセス ポイントに透過的にこのプロファイルが伝達されます。（図 8-1 を参照）。

図 8-1　　wIPS プロファイルの設定および更新

NCS で wIPS プロファイルへの設定変更が行われ、一連のモビリティ サービス エンジンおよびコントローラに適用される場合、次のようになります。

1. NCS で設定プロファイルが変更され、バージョン情報が更新されます。
2. XML ベースのプロファイルがモビリティ サービス エンジンで実行する wIPS エンジンに適用されます。この更新は、SOAP/XML プロトコルを介して行われます。
3. モビリティ サービス エンジン上の wIPS は、NMSP を使用して設定プロファイルを適用することによって、そのプロファイルに関連付けられている各コントローラを更新します。
4. コントローラは更新された wIPS プロファイルを受け取り、それを NVRAM に保存し（以前のすべてのバージョンのプロファイルを置き換える）、CAPWAP 制御メッセージを使用して、更新されたプロファイルをそれに関連付けられた wIPS アクセス ポイントに伝播します。
5. wIPS モード アクセス ポイントはコントローラから更新されたプロファイルを受け取り、その wIPS ソフトウェア エンジンに変更を適用します。

この項では、次のトピックを扱います。

ガイドラインと制限事項

- wIPS モニタ モードをサポートしているのは、Cisco Aironet 1130、1140、1240、1250、3502E、および 3502I シリーズのアクセス ポイントだけです。
- wIPS サブモードがサポートされるのは、アクセス ポイント モードがモニタ、ローカル、または HREAP の場合だけです。ただし、1130 および 1240 アクセス ポイントの場合、wIPS はモニタ モードだけでサポートされます。

wIPS モニタ モードのアクセス ポイントの設定

wIPS モニタ モードで動作するようにアクセス ポイントを設定するには、次の手順に従います。

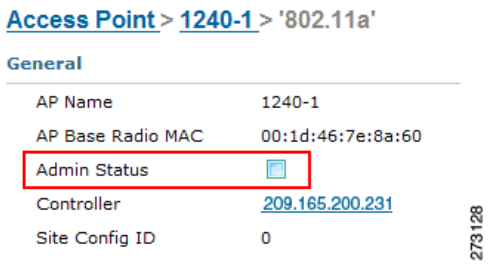
ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[802.11a] または [802.11b/g] 無線リンクをクリックします（図 8-2 を参照）。

図 8-2　[Configure] > [Access Points] > [Radio]

ステップ 3　[Access Point] ページで、[Admin Status] チェックボックスをオフにして無線を無効にします。

図 8-3　[Access Points] > [Radio]



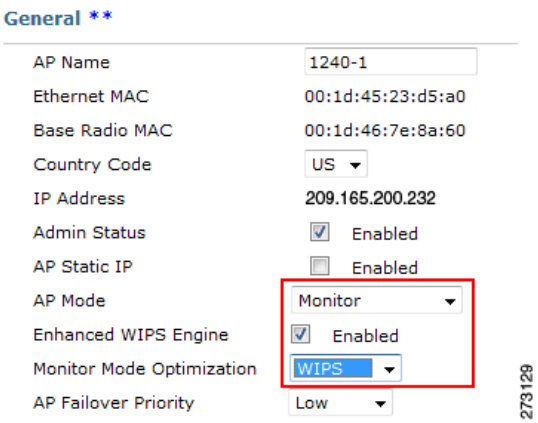
ステップ 4　[Save] をクリックします。

（注）　wIPS モニタ モードに設定されるアクセス ポイント上の各無線について、これらの手順を繰り返します。

ステップ 5　無線が無効になると、[Configure] > [Access Points] の順に選択し、無効にした無線のアクセス ポイントの名前をクリックします。

ステップ 6　アクセス ポイントのダイアログボックスで、[AP Mode] ドロップダウン リストから [Monitor] を選択します（図 8-4 を参照）。

図 8-4　[Configure] > [Access Points] > アクセス ポイントの詳細



ステップ 7　[Enhanced WIPS Engine] の [Enabled] チェックボックスをオンにします。

ステップ 8　[Monitor Mode Optimization] ドロップダウン リストから [WIPS] を選択します。

ステップ 9　[Save] をクリックします。

ステップ 10　アクセス ポイントをリブートするように求められたら、[OK] をクリックします。

ステップ 11　アクセス ポイント無線を再度有効にするには、[Configure] > [Access Points] の順に選択します。

ステップ 12　該当するアクセス ポイント無線をクリックします（図 8-5 を参照）。

図 8-5　[Configure] > [Access Points] > [Radio]

ステップ 13　[Radio Detail] ページで、[Admin Status] の [Enabled] チェックボックスをオンにします。

ステップ 14　[Save] をクリックします。

wIPS モニタ モードに設定した各アクセス ポイントおよびその各無線について、この手順を繰り返します。

wIPS プロファイルの設定

デフォルトで、モビリティ サービス エンジンと対応する wIPS アクセス ポイントは NCS からデフォルトの wIPS プロファイルを継承します。このプロファイルは、デフォルトで有効にされている大部分の攻撃アラームによってあらかじめ調整されており、wIPS アクセス ポイントと同じ RF グループ内のアクセス ポイントに対する攻撃を監視します。このように、システムは WLAN インフラストラクチャと wIPS アクセス ポイントの両方が同じコントローラ上に混合されている統合ソリューションを利用する構成モデルに対する攻撃を監視するようにあらかじめ設定されています。

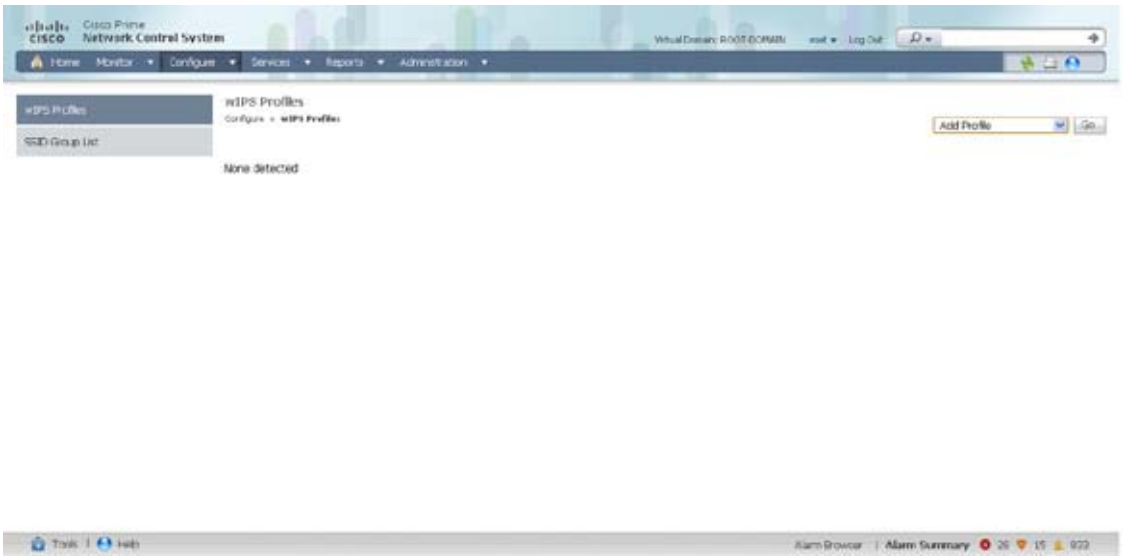
（注）　次の設定手順の一部は*オーバーレイだけ*としてマークされており、Autonomous や完全に個別のコントローラベースの WLAN などの既存の WLAN インフラストラクチャを監視するように適応型 wIPS ソリューションを導入している場合にだけ実行されます。

wIPS プロファイルを設定するには、次の手順に従います。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。

[wIPS Profiles] ページが表示されます（図 8-6 を参照）。

図 8-6　[wIPS Profiles] > プロファイル リスト



ステップ 2　[Select a command] ドロップダウン リストから、[Add Profile] を選択し、[Go] をクリックします。

ステップ 3　[Profile Parameters] ダイアログボックスで、[Copy From] ドロップダウンリストからプロファイル テンプレートを選択します。

（注）　適応型 wIPS には一連のプロファイル テンプレートがあらかじめ定義されており、お客様はそれらをベースとして使用して、独自のカスタム プロファイルを作成できます。各プロファイルは、そのプロファイルで有効な特定のアラームと同様に、特定の業務または用途に合わせて作成されています。

（注）　デフォルト プロファイルは編集できません。

（注）　プロファイルをコントローラに適用するために NMSP セッションがアクティブなことを確認します。

ステップ 4　プロファイルを選択し、プロファイル名を入力したら、[Save and Edit] をクリックします。

ステップ 5　（任意）[SSID Group List] ページで SSID を設定します。

デフォルトで、ローカル ワイヤレス LAN インフラストラクチャ（同じ RF グループ名を持つ AP によって定義された）に対して仕掛けられた攻撃が監視されます。オーバーレイ構成モデルで構成する場合など、他のネットワークに対する攻撃を監視させる必要がある場合は、SSID グループ機能を使用する必要があります。

（注）　この手順が必要ない場合は、単に [Next] をクリックします。

a.　[MyWLAN] チェックボックスをオンにし、ドロップダウン リストから [Edit Group] を選択して、[Go] をクリックします。

b. 監視する SSID を入力します。

c. SSID 名を入力し（複数の名前を入力する場合は 1 つのスペースで区切る）、**[Save]** をクリックします。

SSID が正常に追加されたことを確認する [SSID Groups] ページが表示されます。

d. [Next] をクリックします。

[Select Policy] および [Policy Rules] 概要ペインが表示されます。

（注）　[Select Policy] ペインで、検出および報告対象の攻撃を有効または無効にすることができます。アラームのしきい値を編集し、フォレンジックを有効にすることもできます。

ステップ 6　検出および報告対象の攻撃を有効または無効にするには、[Select Policy] ペインでその攻撃タイプの横にあるチェックボックスをオンにします。

ステップ 7　プロファイルを編集するには、攻撃タイプの名前（DoS：アソシエーション フラッドなど）をクリックします。

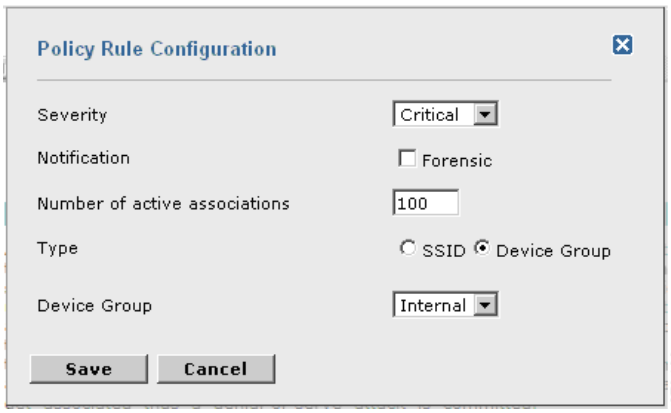
その攻撃タイプの設定ペインが、ポリシー ルールの説明の上の右側のペインに表示されます。

ステップ 8　ポリシー ルールを変更するには、次の手順に従います。

a. [Policy Rules] ペインで、ポリシー ルールの横にあるチェックボックスをオンにし、[Edit] をクリックします。

[Policy Rule Configuration] ダイアログボックスが表示されます（図 8-7 を参照）。

図 8-7　[Policy Rule Configuration] ダイアログボックス



b. アラームの重大度を選択します。

c. このアラームのパケットをキャプチャする場合は、[Forensic] チェックボックスをオンにします。

d. 必要に応じて、アクティブなアソシエーションの数を変更します。（この値はアラーム タイプによって異なります）。

e. 攻撃を監視する WLAN インフラストラクチャのタイプ（[SSID] または [Device Group]）を選択します。

1. [SSID] を選択した場合は、ステップ 9 に進みます。
2. [Device Group] を選択した場合は、ステップ 10 に進みます。

（注）　[Device Group]（[Type]）および [Internal] はデフォルトです。*Internal* は、同じ RF グループ内のすべてのアクセス ポイントを示します。タイプに [SSID] を選択すると、オーバーレイ構成に一般的な個別ネットワークを監視できます。

ステップ 9　（任意）オーバーレイ構成に限り、SSID のポリシー ルールを追加するには、以下の手順に従います。

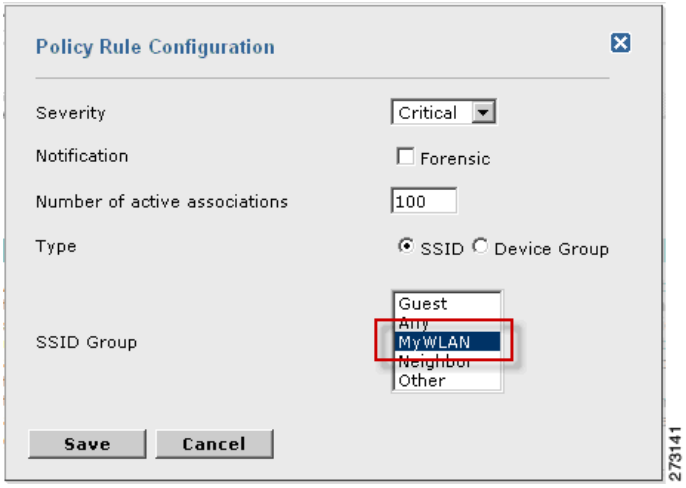
a. ポリシー ルールを追加するには、[Add] をクリックします（図 8-8 を参照）。

図 8-8　　ポリシー ルールの追加

b. [Policy Rule Configuration] ダイアログボックスで、[SSID Group] リストから [MyWLAN] を選択します（図 8-9 を参照）。

（注）　タイプに SSID がすでに選択されています。

図 8-9　　SSID の [Policy Rule Configuration] ダイアログボックス

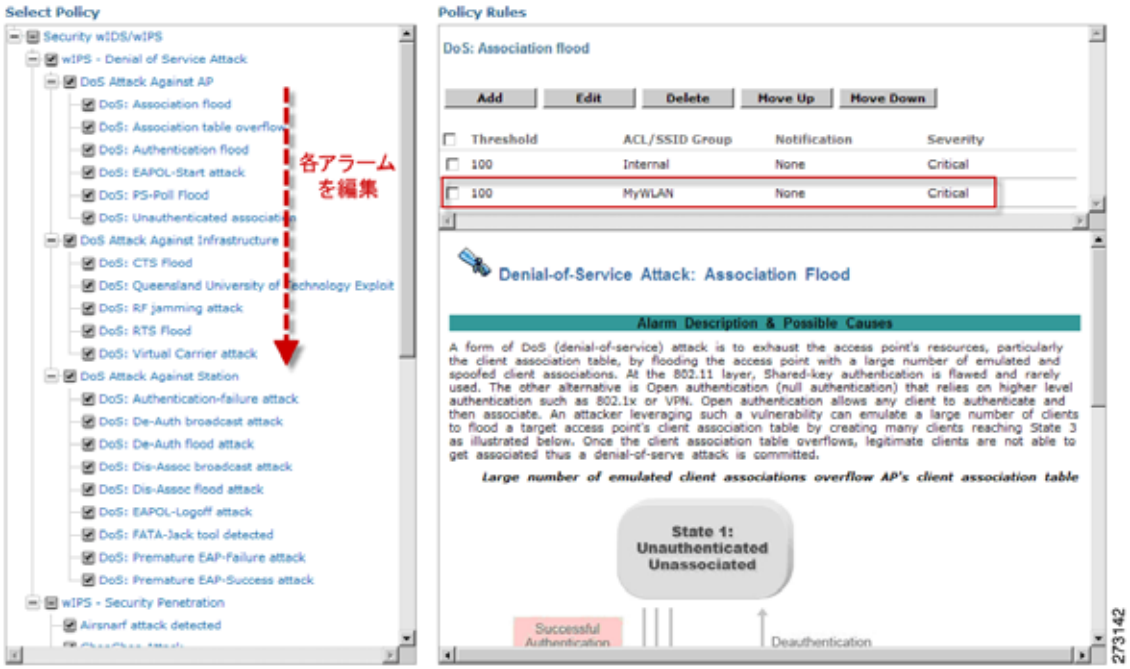


c. すべての変更が完了したら、[Save] をクリックします。

d. 各ポリシー ルールを変更します。すべての変更が完了したら、ステップ 10 に進みます。（図 8-10 を参照）。

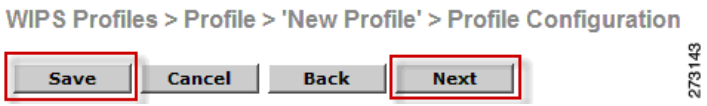
（注）　SSID によって別の WLAN インフラストラクチャを監視するようにシステムを設定する場合、監視するすべてのポリシー ルールごとに変更する必要があります。個別の各アラームに、システムで以前に作成した SSID グループに対する攻撃を監視するように定義したポリシー ルールを作成する必要があります。

図 8-10　SSID モニタリングに関するポリシー ルールの編集



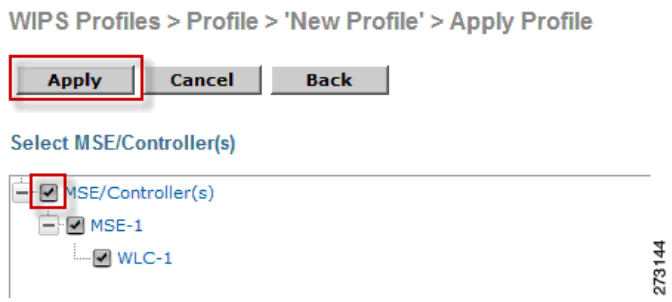
ステップ 10　[Profile Configuration] ダイアログボックスで、[Save] をクリックしてプロファイル（SSID またはデバイス グループ）を保存します。[Next] をクリックします（図 8-11 を参照）。

図 8-11　[Profile Configuration] ダイアログボックス



ステップ 11　プロファイルを適用する MSE/ コントローラの組み合わせを選択して、[Apply] をクリックします（図 8-12 を参照）。

図 8-12　[Apply Profile] ダイアログボックス



CHAPTER 9

システムとサービスのモニタリング

この章では、アラーム、イベント、およびログの設定と表示によるモビリティ サービス エンジンのモニタ方法、システムの使用率および要素（タグ、クライアント、不正クライアント、干渉、およびアクセス ポイント）のカウントについてのレポートの生成方法について説明します。

また、NCS を使用して、クライアント（有線と無線）、タグ、チェックポイント、および Wi-Fi TDOA 受信機をモニタする方法についても説明します。

この章は、次の内容で構成されています。

アラームの処理

この項では、NCS を使用したモビリティ サービス エンジンのアラームとイベントの表示、割り当て、およびクリア方法について説明します。また、アラーム通知（All、Critical、Major、Minor、Warning）の定義方法、およびそれらのアラーム通知を電子メール送信する方法の詳細についても説明します。

この項では、次のトピックを扱います。

ガイドラインと制限事項

重大度が [Clear] になると、アラームは 30 日経過後に NCS から削除されます。

アラームの表示

モビリティ サービス エンジンのアラームを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] の順に選択します。

ステップ 2　ナビゲーション バーにある [Advanced Search] リンクをクリックします。アラーム用の設定可能な検索ダイアログボックスが表示されます。

ステップ 3　[Search Category] ドロップダウン リストから [Alarms] を選択します。

ステップ 4　[Severity] ドロップダウン リストから、[Severity of Alarms] を選択します。オプションは、[All Severities]、[Critical]、[Major]、[Minor]、[Warning]、または [Clear] です。

ステップ 5　[Alarm Category] ドロップダウン リストから、[Mobility Service] を選択します。

ステップ 6　[Condition] コンボ ボックスから [Condition] を選択します。または、コンボ ボックスの [Condition] に条件を入力することもできます。

ステップ 7　[Time Period] ドロップダウン リストから、アラームを確認するタイム フレームを選択します。

オプションの範囲は、分単位（5、15、および 30）から、時間単位（1 ～ 8）、日数単位（1 ～ 7）までです。すべてを表示するには、[Any time] を選択します。

ステップ 8　[Alarm Summary] ページの認知しているアラームとそれぞれのカウントを除外するには、[Acknowledged State] チェックボックスをオンにします。

ステップ 9　[Alarm Summary] ページの割り当て済みのアラームとそれぞれのカウントを除外するには、[Assigned State] チェックボックスをオンにします。

ステップ 10　[Items per page] ドロップダウン リストから、各ページに表示するアラーム数を選択します。

ステップ 11　後で使用するために検索条件を保存するには、[Save Search] チェックボックスをオンにして、検索の名前を入力します。

（注）　その後は、[Saved Search] リンクをクリックすることで、その検索を開始できます。

ステップ 12　[Go] をクリックします。[alarms summary] ダイアログボックスが表示され、検索結果が表示されます。

（注）　アラームをソートするには、列見出し（[Severity]、[Failure Source]、[Owner]、[Date/Time]、[Message]、および [Acknowledged]）をクリックします。

ステップ 13　ステップ 2 からステップ 12 を繰り返して、モビリティ サービス エンジンの Context-Aware Service 通知を確認します。ステップ 5 で、アラーム カテゴリとして「**Context Aware Notifications**」と入力します。

MSE アラーム詳細の表示

MSE アラームの詳細を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] の順に選択します。

ステップ 2　[Failure Source] 列にある MSE をクリックして、特定の MSE のアラーム詳細にアクセスします。

または、[Services] > [Services] > [MSE Name] > [System] > [Status] > [NCS Alarms] ページの順に選択し、[Failure Source] 列にある特定の MSE 項目をクリックして、特定の MSE のアラーム詳細にアクセスします（図 9-1 を参照）。

図 9-1　　MSE アラーム

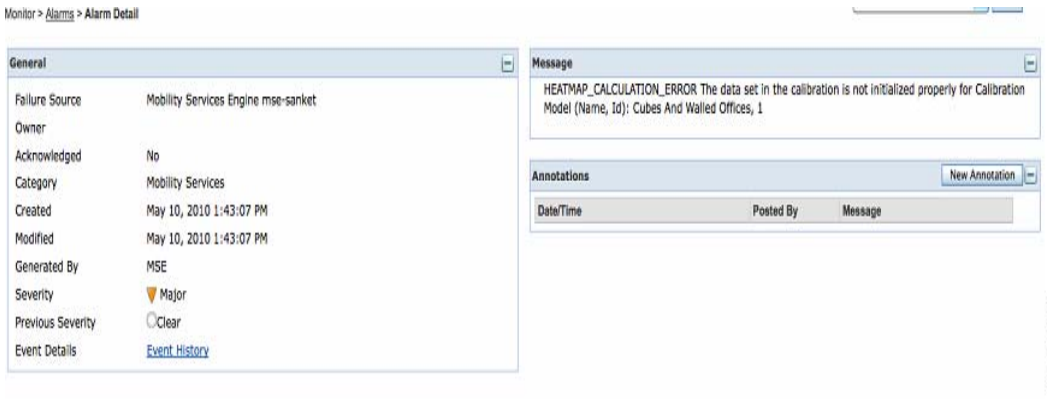


表 9-1 に、MSE の [Alarm Detail] ページの各種フィールドを示します。

表 9-1　　[General] パラメータ

フィールド	説明
[Failure Source]：アラーム検出デバイス	アラームを生成した MSE。
Owner	このアラームの担当者の名前または空欄。
Acknowledged	担当ユーザがこのアラームを認知しているかどうかを示します。
Category	アラームのカテゴリ。アラーム カテゴリは、MSE のモビリティ サービスです。
Created	アラームが作成された日時（月、日、年、時、分、秒、AM/PM）。
Modified	アラームが最後に変更された日時（月、日、年、時、分、秒、AM/PM）。
Generated By	このフィールドは MSE と表示されます。
Severity	セキュリティのレベル：Critical（重大）、Major（やや重大）、Minor（比較的重大でない）、Warning（警告）、Clear（クリア）、Info（通知）が色分けして表示されます。
Previous Severity	Critical（重大）、Major（やや重大）、Minor（比較的重大でない）、Warning（警告）、Clear（クリア）、Info（通知）が 色分けして表示されます。

（注）　全般情報は、アラームのタイプによって異なる場合があります。たとえば、一部のアラーム詳細には、ロケーションおよびスイッチ ポート トレーシング情報が含まれる場合があります。

- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。注釈は [Annotations] 表示ページに表示されます。
- [Messages]：アラームに関する情報が表示されます。
- [Audit Report]：クリックして、設定監査アラームの詳細を表示します。このレポートは、設定監査アラームにだけ使用できます。

  監査の矛盾が設定グループに施行されると、設定監査アラームが生成されます。

  （注）　施行が失敗すると、設定グループに重大なアラームが生成されます。施行が成功すると、設定グループに比較的重大でないアラームが生成されます。

  アラームには監査レポートへのリンクがあり、各コントローラの矛盾のリストを表示できます。

- [Event History]：[MSE Alarm Events] ページを開き、このアラームのイベントを表示します。アラーム ページが複数ある場合は、ページ上部にページ番号とその両側に他のページへ移動するためのスクロール矢印が表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

Select a Command

[Select a command] ドロップダウン リストからは、次の機能にアクセスできます。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択したアラームをクリアします。

  （注）　重大度が [Clear] になると、アラームは 30 日経過後に NCS から削除されます。

- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。アラームは NCS に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。
- [UnAcknowledge]：すでに認知しているアラームの認知を解除できます。
- [Email Notification]：[All Alarms] > [Email Notification] ページを開き、電子メール通知を表示して設定します。
- [Event History]：[Monitor] > [Events] ページを開き、このアラームのイベントを表示します。

アラームの割り当てと割り当て解除

アラームの割り当ておよび割り当て解除を行うには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] の順に選択して、[Alarms] ページを開きます。

ステップ 2　対応するチェックボックスをオンにすることで、自分に割り当てるアラームを選択します。

（注）　自分に割り当てられているアラームを割り当て解除するには、該当アラームの隣にあるボックスをオフにします。他の人に割り当てられているアラームの割り当ては解除できません。

ステップ 3　[Select a command] ドロップダウン リストから、[Assign to Me]（または [Unassign]）を選択します。[Go] をクリックします。

アラームの削除とクリア

アラームを削除すると、アラームは NCS によってデータベースから削除されます。アラームをクリアすると、NCS データベースには残りますが、[Clear] 状態になります。アラームは、その原因となった状況が存在しなくなったときにクリアする必要があります。

モビリティ サービス エンジンからアラームを削除またはクリアするには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] の順に選択して、[Alarms] ページを開きます。

ステップ 2　対応するチェックボックスをオンにして、削除またはクリアするアラームを選択します。

ステップ 3　[Select a command] ドロップダウン リストから [Delete] または [Clear] を選択します。[Go] をクリックします。

電子メール アラーム通知

NCS では、特定の電子メール アドレスに電子メール通知を送信できます。電子メール経由で通知を送信することで、必要な場合に迅速なアクションをとることができます。

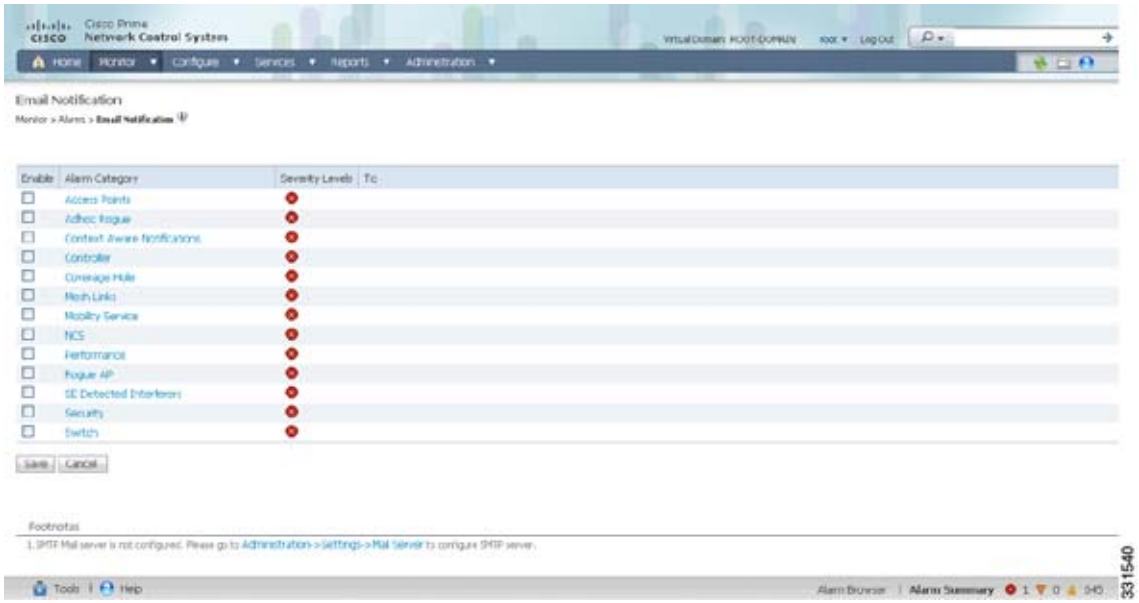
自分に電子メールで送信されるアラーム重大度のタイプ（Critical、Major、Minor、および Warning）を選択できます。

アラーム通知を送信するには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Email Notification] を選択します。[Go] をクリックします。[Email Notification] ページが表示されます（図 9-2 を参照）。

図 9-2　[All Alarms > Email Notification] ページ



（注）　SMTP メール サーバは、電子メール通知の対象となる電子メール アドレスを入力する前に定義しておく必要があります。[Administrator] > [Settings] > [Mail Server Configuration] の順に選択して、適切な情報を入力します。

ステップ 3　[Mobility Service] の隣にある [Enabled] チェックボックスをオンにします。

（注）　[Mobility Service] アラーム カテゴリを有効にすると、モビリティ サービス エンジンとロケーション アプライアンスに関連するすべてのアラームが定義済みの電子メール アドレスに送信されます。

ステップ 4　[Mobility Service] リンクをクリックします。モビリティ サービス エンジンに報告されるアラーム重大度のタイプを設定するページが表示されます。

ステップ 5　電子メール通知を送信するすべてのアラーム重大度のタイプの隣にあるチェックボックスをオンにします。

ステップ 6　[To] テキスト ボックスに、電子メール通知を送信する 1 つまたは複数の電子メール アドレスを入力します。電子メール アドレスはカンマで区切ります。

ステップ 7　[OK] をクリックします。

[Alarms > Notification] ページに戻ります。報告されたアラーム重大度のレベルに対する変更と電子メール通知の受信者の電子メール アドレスが表示されます。

イベントの使用

NCS を使用して、モビリティ サービス エンジンおよびロケーション通知イベントを確認できます。イベントは、それぞれの重大度（Critical、Major、Minor、Warning、Clear、Info）およびイベント カテゴリに基づき検索して表示できます。

ロケーション通知イベントの表示

ロケーション通知イベントを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Events] を選択します。

ステップ 2　[Events] ページでは、次の操作を実行できます。

- 特定の要素のイベントを表示する場合に、その IP アドレス、名前、WLAN SSID、または　MAC アドレスがわかっている場合は、ナビゲーション バーの [Search] テキスト ボックスにその値を入力します。[Search] をクリックします。
- 重大度やカテゴリでイベントを表示するには、ナビゲーション バーで [Advanced Search] をクリックして、[Severity] および [Event Category] ドロップダウン リスト ボックスから適切なオプションを選択します。[Go] をクリックします。

ステップ 3　検索条件に一致するイベントが見つかると、それらのイベントが一覧表示されます。

（注）　イベントの詳細を表示するには、イベントに関連付けられている [Failure Source] をクリックします。また、イベントの概要を各列見出しで並べ替えることができます。

ログの操作

この項では、ロギング オプションの設定方法と、ログ ファイルのダウンロード方法について説明します。

この項では、次のトピックを扱います。

ガイドラインと制限事項

- ログ レベルから適切なオプションを選択する際には、Cisco TAC 担当者から [Error] と [Trace] のみ使用するように指示があった場合は、指示に従ってください。
- 詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

ロギング オプションの設定

NCS を使用して、ログに記録するメッセージのタイプとログ レベルを指定できます。

ロギング オプションを設定するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　設定するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] メニューから [Logs] を選択します。選択されているモビリティ サービス エンジンのロギング オプションが表示されます。

ステップ 4　[Logging Level] ドロップダウン リストから適切なオプションを選択します。

ロギング オプションは、[Off]、[Error]、[Information]、および [Trace] の 4 つです。

ログ レベルが [Error] またはこれよりも上のレベルに設定されているログ レコードはすべて、新しいエラー ログ ファイル locserver-error-%u-%g.log に記録されます。これは、ロケーション サーバの locserver-%u-%g.log ログ ファイルとともに維持される追加のログ ファイルです。このエラー ログ ファイルには、[Error] レベルのログとそのコンテキスト情報が記録されます。コンテキスト情報には、当該エラーよりも前の 25 ログ レコードが含まれています。最大 10 のエラー ログ ファイルを維持できます。各ログ ファイルの最大許容サイズは 10 MB です。

注意　[Error] と [Trace] は、Cisco Technical Assistance Center（TAC）担当者の指示がある場合にだけ使用してください。

ステップ 5　イベントのロギングを開始する各要素の隣にある [Enabled] チェックボックスをオンにします。

ステップ 6　[Advanced Parameters] の [Enable] チェックボックスをオンにして、詳細デバッグを有効にします。デフォルトでは、このオプションは無効になっています。

注意　詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

ステップ 7　サーバからログ ファイルをダウンロードするには、[Download Logs] をクリックします。詳細については、「ログ ファイルのダウンロード」（P.9-9）を参照してください。

ステップ 8　[Log File] グループ ボックスに、以下の情報を入力します。

- モビリティ サービス エンジンで維持するログ ファイルの数。モビリティ サービス エンジンで維持できるログ ファイルの数は 5 ～ 20 です。
- 最大ログ ファイル サイズ（MB 単位）。ログ ファイルのサイズは 10 ～ 50 MB です。

ステップ 9　[MAC Address Based Logging] ページで、次の手順を実行します。

- [Enable] チェックボックスをオンにし、MAC アドレス ロギングを有効にします。デフォルトでは、このオプションは無効になっています。
- ロギングを有効にする 1 つ以上の MAC アドレスを追加します。また、以前に追加した MAC アドレスを削除できます。削除するには、リストから MAC アドレスを選択して [Remove] をクリックします。

MAC アドレスに基づくロギングの詳細については、「MAC アドレスに基づくロギング」（P.9-9）を参照してください。

ステップ 10　[Save] をクリックして変更を適用します。

MAC アドレスに基づくロギング

この機能では、指定されている MAC アドレスのエンティティ固有のログ ファイルを作成できます。ログ ファイルは次に示すパスの locserver ディレクトリ内に作成されます。

/opt/mse/logs/locserver

一度に最大で 5 つの MAC アドレスをログに記録できます。MAC アドレス aa:bb:cc:dd:ee:ff のログ ファイルの形式は次のとおりです。

macaddress-debug-aa-bb-cc-dd-ee-ff.log

1 つの MAC アドレスに対して最大 2 つのログ ファイルを作成できます。2 つのログ ファイルは、1 つのメインと 1 つのバックアップまたはロールオーバー ログ ファイルで構成できます。

MAC ログ ファイルの最小サイズは 10 MB です。最大許容サイズは、MAC アドレスあたり 20 MB です。24 時間以上更新されていない MAC ログ ファイルはプルーニングされます。

ログ ファイルのダウンロード

モビリティ サービス エンジン ログ ファイルを解析する必要がある場合は、NCS を使用してログ ファイルをシステムにダウンロードできます。NCS はログ ファイルが含まれている .zip ファイルをダウンロードします。

ログ ファイルが含まれている .zip ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　ステータスを表示するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[Logs] を選択します。

ステップ 4　[Download Logs] をクリックします。

ステップ 5　[File Download] ダイアログボックスの指示に従い、ファイルを表示するか、または .zip ファイルをシステムに保存します。

レポートの生成

NCS では、さまざまな種類のレポートを生成できます。この項では、NCS Report Launch Pad を使用して、Context Aware レポートを生成する方法について説明します。デフォルトでは、レポートは NCS サーバに保存されます。

レポート基準を定義したら、今後の診断で使用するためにレポートを保存し、臨時的に、またはスケジュール ベースでレポートを実行できます。

レポートの次の基準を定義できます。

- モニタする 1 つまたは複数のモビリティ サービス エンジン
- レポートの生成頻度

- グラフ上でのデータの表示方法
- レポートを電子メールで送信するか、ファイルにエクスポートするか

この項では、次のトピックを扱います。

- 「デバイス使用率レポートの作成」（P.9-10）
- 「保存した使用率レポートの表示」（P.9-12）
- 「スケジュールされた使用率の実行の表示」（P.9-12）

デバイス使用率レポートの作成

モビリティ サービス エンジンのデバイス使用率レポートを作成するには、次の手順を実行します。

ステップ 1　[Reports] > [Report Launch Pad] の順に選択します。

ステップ 2　[Device] > [Utilization] の順に選択します。

ステップ 3　[New] をクリックします。[Utilization Report Details] ページが表示されます。

ステップ 4　[Report Details] ページで、次の [Settings] パラメータを入力します。

（注）　一部のパラメータは、レポート タイプによっては機能することも、機能しないこともあります。

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- [Report Type]：デフォルトでは、レポート タイプは MSE が選択されます。
- [Report By]：ドロップダウン リストから該当する [Report By]（レポート単位）のカテゴリを選択します。カテゴリはレポートごとに異なります。各レポートの [Report By] カテゴリについては、特定のレポートの項を参照してください。
- [Report Criteria]：このパラメータを指定すると、事前に選択した [Report By] に応じて、結果をソートできます。[Edit] をクリックして、[Filter Criteria] ページを開きます。
- [Connection Protocol]：[All Clients]、[All Wired (802.3)]、[All Wireless (802.11)]、[802.11a/n]、[802.11b/g/n]、[802.11a]、[802.11b]、[802.11g]、[802.11n (5 GHz)]、または [802.11n (2.4 GHz)] からいずれかのプロトコルを選択します。
- [SSID]：[All SSIDs] がデフォルト値です。
- [Reporting Period]：時間単位、週単位、または特定の日時にデータを収集するようにレポートを定義できます。選択したレポート期間のタイプは、x 軸に表示されます。

（注）　レポート期間には、12 時間表記ではなく 24 時間表記が使用されます。たとえば、午後 1 時の場合は、**13 時**を選択します。

ステップ 5　[Schedule] グループ ボックスで、[Enable Schedule] チェックボックスをオンにします。

ステップ 6　[Export Report] ドロップダウン リストから、レポート形式（[CSV] または [PDF]）を選択します。

ステップ 7　レポートの保存先として、[File] または [Email] を選択します。

- [File] オプションを選択する場合は、先に [Administration > Settings > Report] ページで保存先パスを定義しておく必要があります。[Repository Path] テキスト ボックスに、ファイルの保存先パスを入力します。
- [Email] オプションを選択する場合は、目的の電子メール アドレスを入力する前に、SMTP メール サーバを定義しておく必要があります。[Administrator] > [Settings] > [Mail Server Configuration] の順に選択して、適切な情報を入力します。

ステップ 8　開始日（MM:DD:YYYY）を入力するか、[calendar] アイコンをクリックして日付を選択します。

ステップ 9　[hour] と [minute] のドロップダウン リスト ボックスを使用して開始時刻を指定します。

ステップ 10　[Recurrence] オプション ボタンを選択して、レポートの実行頻度を決定します。次の値が可能です。

- No Recurrence
- Hourly
- Daily
- Weekly
- Monthly

（注）　曜日は [Weekly] オプションを選択した場合のみページ上に表示されます。

ステップ 11　ステップ 1 からステップ 10 まで完了したら、次のいずれかを実行します。

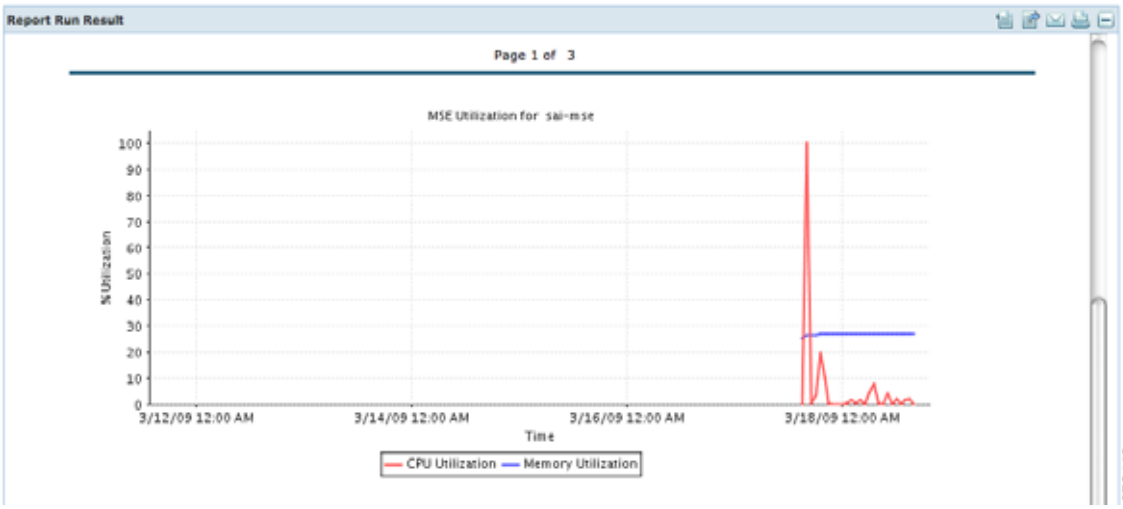
- [Save] をクリックして編集を保存します。指定した時刻にレポートが実行され、[Schedule] グループ ボックスでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
- [Save and Run] をクリックして、変更内容を保存し、レポートをすぐに実行します。レポートは、そのレポートのスケジュールされた実行が保留中であっても実行されます。結果はページの一番下に表示されます。レポートは指定した時刻にも実行され、[Schedule] グループ ボックスでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
  - 結果のページで、[Cancel] をクリックして、定義済みのレポートをキャンセルします。
- レポートをすぐに実行して結果を [NCS] ページで確認するには、[Run Now] をクリックします。レポートは、そのレポートのスケジュールされた実行が保留中であっても実行されます。結果はページの一番下に表示されます。入力したレポート条件を保存する場合は [Save] をクリックします。

（注）　[Run Now] をクリックして、保存する前に定義済みのレポート条件を確認したり、必要に応じてレポートを実行したりすることもできます。

結果はページの一番下に表示されます（図 9-3 を参照）。

（注）　次の例には、CPU とメモリの使用率レポートのみ表示されています（図 9-3 を参照）。

図 9-3　[Devise] > [MSE Utilization] > [Results]



ステップ 12　[Save] または [Save and Run] オプションを選択した場合は、[Reports] > [Saved Reports] の順に選択します（または、レポートが未実行で、実行がスケジュールされている場合は、[Reports] > [Scheduled Runs] の順に選択します）。[Utilization Reports Summary] ページが表示されます。

スケジュールされているレポートは、「enabled」として表示され、次の実行スケジュール日が表示されます。

実行済みで次の実行がスケジュールされていないレポートは、「expired」として表示されます。

実行済みで再度実行するようにスケジュールされているレポートは、「disabled」として表示されます。

ステップ 13　レポートを有効化、無効化、または削除するには、そのレポート タイトルの隣にあるチェックボックスをオンにして、適切なオプションをクリックします。

保存した使用率レポートの表示

保存したレポートをダウンロードするには、次の手順を実行します。

ステップ 1　[Reports] > [Saved Reports] の順に選択します。

ステップ 2　レポートの [Download] アイコンをクリックします。レポートがダウンロードされ、定義済みのディレクトリに保存されるか、電子メールで送信されます。

スケジュールされた使用率の実行の表示

スケジュールされたレポートのステータスを確認するには、次の手順を実行します。

ステップ 1　[Reports] > [Scheduled Runs] の順に選択します。

ステップ 2　[History] アイコンをクリックして、レポートの最終実行日を確認します。

ステップ 3　レポートの [Download] アイコンをクリックします。レポートがダウンロードされ、定義済みのディレクトリに保存されるか、電子メールで送信されます。

wIPS のセキュリティ レポートとアラーム

wIPS のセキュリティ レポートとアラームを確認、変更、または作成できます。

（注） セキュリティ レポートには、Autonomous アクセス ポイントのステータスは表示されません。

次の選択肢があります。

- [Adaptive wIPS Alarms]：モニタ モードのアクセス ポイントで wIPS に報告されるアラームです。
- [Adaptive wIPS Top 10 AP]：モニタ アクセス ポイントで報告された最新の 10 イベントが一覧表示されます。
- [Adhoc Rogue Event]：選択した時間帯に NCS が受信したアドホック イベントがすべて表示されます。
- [Adhoc Rogues]：選択した時間帯に更新されたアドホックがすべて表示されます。
- [New Rogue APs]：選択した時間帯に検出された不正アクセス ポイントが表形式ですべて表示されます。選択した時間内に検出された新しい不正アクセス ポイントを示します。作成時刻は、不正アクセス ポイントが最初に検出された時刻です。
- [New Rogue AP Count]：選択した時間帯に検出された不正アクセス ポイントがグラフ形式ですべて表示されます。
- [Rogue APs]：ネットワーク内のアクティブな不正アクセス ポイントと選択した時間帯に更新された不正アクセス ポイントがすべて表示されます。NCS は、検出された不正アクセス ポイントの更新イベントを受信します。
- [Rogue APs Event]：NCS が受信したすべてのイベントが表示されます。属性が変更されるか、または新しい不正アクセス ポイントが検出されると、最新の不正アクセス ポイント検出情報がコントローラから送信されます。

（注） このレポートは、正式には Rogue Detected by AP と呼ばれます。

- [Security Summary]：アソシエーション失敗回数、不正なアクセス ポイント数、不正なアドホック数、不正なアクセス ポイント接続数、または 1 か月以上にわたる切断が表示されます。
- [Save and Run] をクリックして、変更内容を保存し、レポートをすぐに実行します。レポートは、そのレポートにアソシエートされているスケジュール時間に関係なく実行され、[Results] タブで確認することができます。また、レポートは指定した時刻に実行され、[Schedule] タブでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
  - 結果のページで、レポートのキャンセルや削除ができます。

この項では、次のトピックを扱います。

- 「wIPS のセキュリティまたはアラームのレポートの新規作成」（P.9-14）
- 「保存した wIPS レポートの表示」（P.9-15）
- 「wIPS レポートの実行スケジュールの表示」（P.9-15）

wIPS のセキュリティまたはアラームのレポートの新規作成

セキュリティ レポートには、wIPS のアクセス ポイントと不正アクセス ポイントに関する多くの詳細が表示されます。

新しいセキュリティ レポートを作成するには、次の手順を実行します。

（注）　この手順またはオプションの中には、レポートによっては必要ないものもあります。

ステップ 1　[Reports] > [Report Launch Pad] の順に選択します。[Report Launch Pad] ページが表示されます。

ステップ 2　[Security] を選択し、左側のペインでいずれかのレポート タイプ（[Adaptive wIPS Top 10 Report Details] など）をクリックします。

ステップ 3　[New] をクリックします。[New report] ページが表示されます。

ステップ 4　[Settings] ペインで、レポートのタイトルを入力します。

ステップ 5　[Report By] は、デフォルトでは [MSE with Adaptive wIPS Service] です。

ステップ 6　[Report Criteria] は常に、特定のモビリティ サービス エンジンか、[All MSEs with Adaptive wIPS Service] です。

ステップ 7　[Edit] をクリックして、[Report Criteria] を追加または変更します。[Filter Criteria] ダイアログボックスが表示されます。

ステップ 8　レポート期間を入力します。時間単位、週単位、または特定の日時にデータを収集するようにレポートを定義できます。選択したレポート期間のタイプは、x 軸に表示されます。

（注）　レポート期間には、12 時間表記ではなく 24 時間表記が使用されます。たとえば、午後 1 時の場合は、13 時を選択します。

ステップ 9　[Schedule] ペインで、[Enable Schedule] チェックボックスをオンにします。

ステップ 10　[Export Report] ドロップダウン リストから、レポート形式（[CSV] または [PDF]）を選択します。

ステップ 11　レポートの保存先として、[File] または [Email] を選択します。

- [File] オプションを選択する場合は、先に [Administration > Settings > Report] ページで保存先パスを定義しておく必要があります。[Repository Path] テキスト ボックスに、ファイルの保存先パスを入力します。
- [Email] オプションを選択する場合は、目的の電子メール アドレスを入力する前に、SMTP メール サーバを定義しておく必要があります。[Administrator] > [Settings] > [Mail Server Configuration] の順に選択して、適切な情報を入力します。

ステップ 12　開始日（MM:DD:YYYY）を入力するか、[calendar] アイコンをクリックして日付を選択します。

ステップ 13　[hour] と [minute] のドロップダウン リストを使用して開始時刻を選択します。

ステップ 14　[Recurrence] オプションのいずれかを選択して、レポートの実行頻度を決定します。

（注）　[Days of the week] チェックボックスは [Weekly] オプション ボタンを選択した場合のみ表示されます。

[Customize Report] オプションを使用して、レポートをカスタマイズすることもできます。[Customize] をクリックして、レポートを生成するのに必要な情報を入力します。

ステップ 15　ステップ 1 からステップ 14 まで完了したら、次のいずれかを実行します。

- [Save] をクリックして編集を保存します。指定した時刻にレポートが実行され、[Schedule] ペインでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
- [Save and Run] をクリックして、変更内容を保存し、レポートをすぐに実行します。レポートは、そのレポートのスケジュールされた実行が保留中であっても実行されます。結果はページの一番下に表示されます。レポートは指定した時刻にも実行され、[Schedule] ペインでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
  - 結果のページで、[Cancel] をクリックして、定義済みのレポートをキャンセルします。
- レポートをすぐに実行して結果を [NCS] ページで確認するには、[Run Now] をクリックします。レポートは、そのレポートのスケジュールされた実行が保留中であっても実行されます。結果はページの一番下に表示されます。入力したレポート条件を保存する場合は [Save] をクリックします。

（注）　[Run Now] をクリックして、保存する前に定義済みのレポート条件を確認したり、必要に応じてレポートを実行したりできます。

結果はページの一番下に表示されます。

ステップ 16　作成する wIPS レポートごとに、ステップ 2 から ステップ 15 までを繰り返します。

保存した wIPS レポートの表示

保存したレポートをダウンロードするには、次の手順を実行します。

ステップ 1　[Reports] > [Saved Reports] の順に選択します。

ステップ 2　[History] アイコンをクリックして、レポートの最終実行日を確認します。

ステップ 3　必要なレポートの [Download] アイコンをクリックします。レポートがダウンロードされ、定義済みのディレクトリに保存されるか、電子メールで送信されます。

wIPS レポートの実行スケジュールの表示

スケジュールされたレポートのステータスを確認するには、次の手順を実行します。

ステップ 1　[Reports] > [Scheduled Runs] の順に選択します。

ステップ 2　[History] アイコンをクリックして、レポートの最終実行日を確認します。

ステップ 3　レポートの [Download] アイコンをクリックします。レポートがダウンロードされ、定義済みのディレクトリに保存されるか、電子メールで送信されます。

（注）　クライアントに複数の IP アドレスがアソシエートされている場合でも、情報を確認するためにそのクライアントの上にカーソルを移動した場合、1 つの IP アドレスのみ表示されます。詳細ページには、すべての IP アドレスが表示されます。表示されるクライアントは、クライアントに設定できる複数の IP アドレス（全体または一部）のいずれかを使用してフィルタリングすることもできます。表示される IP アドレスは、検索文字列と最も一致しているものです。

MSE でのクライアントのサポート

NCS の Advanced Search 機能を使用して、特定のカテゴリおよびフィルタに基づいて、クライアントリストを絞り込むことができます。詳細については、「Using the Search Feature」（P.2-34）を参照してください。[Show] ドロップダウン リストを使用して、現在のリストをフィルタリングすることもできます。詳細については、「Filtering Client and Users」（P.10-11）を参照してください。

この項では、次のトピックを扱います。

- 「IPv6 アドレスによる MSE 上の NCS のワイヤレス クライアントの検索」（P.9-16）
- 「MSE で検出されたクライアントの表示」（P.9-17）

IPv6 アドレスによる MSE 上の NCS のワイヤレス クライアントの検索

（注）　このリリースでは、ワイヤレス クライアントだけが IPv6 アドレスを使用します。

NCS の Advanced Search 機能を使用して、MSE の配置されたクライアントを検索するには、次の手順を実行します。

ステップ 1　NCS UI の右上隅にある [Advanced Search] をクリックします。

ステップ 2　[Search Category] ドロップダウン リストから検索カテゴリとして [Clients] を選択します。

ステップ 3　[Media Type] ドロップダウン リストから、[Wireless Clients] を選択します。

（注）　メディア タイプとして [Wireless Clients] を選択した場合だけ、[Wireless Type] ドロップダウン リストが表示されます。

ステップ 4　[Wireless Type] ドロップダウン リストから、[All]、[Lightweight]、または [Autonomous Clients] のうちいずれかのタイプを選択します。

ステップ 5　[Search By] ドロップダウン リストから、[IP Address] を選択します。

（注）　IP アドレスによるクライアントの検索は、IP アドレス全体または一部を対象にできます。各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

ステップ 6　[Clients Detected By] ドロップダウン リストから、[clients detected by MSE] を選択します。

コントローラと直接通信することで、MSE の Context-Aware Service で検索されるクライアントが表示されます。

ステップ 7　[Last detected within] ドロップダウン リストから、クライアントが検出された時間帯を選択します。

ステップ 8　[Client IP Address] テキスト ボックスにクライアント IP アドレスを入力します。IPv6 アドレスの一部または全体を入力できます。

（注）　IPV4 アドレスを使用して、MSE 上で NCS のクライアントを検索している場合は、[Client IP address] テキスト ボックスに IPV4 アドレスを入力します。

ステップ 9　[Client States] ドロップダウン リストから、クライアントの状態を選択します。ワイヤレス クライアントに指定できる値は、[All States]、[Idle]、[Authenticated]、[Associated]、[Probing]、または [Excused] です。 有線クライアントに指定できる値は、[All States]、[Authenticated]、および [Associated] です。

ステップ 10　[Posture Status] ドロップダウン リストからポスチャ ステータスを選択すると、デバイスがクリーンであるかどうかを判別します。指定できる値は、[All]、[unknown]、[Passed]、および [Failed] です。

ステップ 11　[CCX Compatible] チェックボックスをオンにすると、Cisco Client Extensions と互換性のあるクライアントを検索します。指定できる値は、[All Versions]、[V1]、[V2]、[V3]、[V4]、[V5]、および [V6] です。

ステップ 12　[E2E Compatible] チェックボックスをオンにすると、エンドツーエンドの互換性のあるクライアントを検索します。指定できる値は、[All Versions]、[V1]、および [V2] です。

ステップ 13　[NAC State] チェックボックスをオンにすると、特定のネットワーク アドミッション コントロール（NAC）の状態で特定されるクライアントを検索します。指定可能な値は、[Quarantine]、[Access]、[Invalid]、および [Not Applicable] です。

ステップ 14　[Include Disassociated] チェックボックスをオンにすると、ネットワーク上には存在しなくなったが、NCS には履歴レコードが残っているクライアントが含まれます。

ステップ 15　[Items per page] ドロップダウン リストから、検索結果ページに表示するレコードの数を選択します。

ステップ 16　[Save Search] チェックボックスをオンにして、選択した検索オプションを保存します。

ステップ 17　[Go] をクリックします。

[Clients and Users] ページに、MSE で検出されたすべてのクライアントが表示されます。

MSE で検出されたクライアントの表示

MSE で検出されたすべてのクライアントを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択して、有線クライアントとワイヤレス クライアントの両方の情報を表示します。

[Client and Users] ページが表示されます。

[Clients and Users] 表にはデフォルトでいくつかの列が表示されます。使用可能な列を追加して表示する場合は、 をクリックし、[Columns] をクリックします。使用可能な列が表示されます。[Clients and Users] 表に表示する列を選択します。列内の任意の場所をクリックすると、その列が選択され、クライアントの詳細が表示されます。

ステップ 2　[Show] ドロップダウン リストから [Clients detected by MSE] を選択して、現在のリストをフィルタリングし、MSE で検出されたクライアントをすべて選択します。

有線とワイヤレスを含む、MSE で検出されたすべてのクライアントが表示されます。

[Clients Detected by MSE] 表では、次のさまざまなパラメータを使用できます。

- [MAC Address]：クライアント MAC アドレス。
- [IP Address]：クライアント IP アドレス。

  [IP Address] 列に表示される IP アドレスは、定義済みの優先順位によって決まります。使用可能な最初の IP アドレスが次の順番で [IP address] テキスト ボックスに表示されます。

  - IPv4 アドレス

  （注）　このリリースでは、ワイヤレス クライアントだけが IPv6 アドレスを使用します。各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

  - IPv6 グローバル固有アドレス。このタイプのアドレスが複数ある場合は、クライアントが受信した最新の IPv6 アドレスが表示されます。ユーザがグローバル IPv6 アドレスを 2 つ持っていても、どちらかが期限切れになっている古いルータ アドバタイズメントによって取得したアドレスである場合があるためです。
  - IPv6 ローカル固有アドレス。複数ある場合は、最新の IPv6 ローカル固有アドレスがクライアントによって使用されます。
  - IPv6 リンク ローカル アドレス。他の IPv6 アドレスが割り当てられる前に、セルフアサインされ、通信に使用されるクライアントの IPv6 アドレス。

  次のようなさまざまな IPv6 アドレス タイプがあります。

  - リンクローカル ユニキャスト：リンクローカル アドレスは、自動アドレス設定、ネイバー探索、ルータが存在しないときなどのために、単一リンクでのアドレス指定に使用するように設計されています。
  - サイトローカル ユニキャスト：サイトローカル アドレスは、グローバル プレフィックスには必要のない、サイト内部でのアドレス指定に使用するように設計されています。
  - 集約可能グローバル ユニキャスト：集約可能グローバル ユニキャスト アドレスは、グローバル ネットワーク内でクライアントを一意に特定します。パブリック IPv4 アドレスと同等です。クライアントは複数の集約可能グローバル ユニキャスト アドレスを持つことができます。
- [IP Type]：クライアントの IP アドレス タイプ。指定できるのは、IPv4、IPv6、またはデュアルスタック（IPv4 アドレスと IPv6 アドレスの両方があるクライアントを表す）です。
  - グローバル固有
  - 固有ローカル
  - リンク ローカル
- [User Name]：802.1x 認証に基づいたユーザ名。ユーザ名を使用しないで接続されたクライアントの場合は [Unknown] と表示されます。
- [Type]：クライアント タイプを示します。
  -  Lightweight クライアントを示します
  -  有線クライアントを示します
  -  Autonomous クライアントを示します
- [Vendor]：OUI から導き出されたデバイス ベンダー。
- [Device Name]：ネットワーク認証デバイス名。たとえば、WLC、スイッチなどです。
- [Location]：接続しているデバイスのマップ位置。
- [VLAN]：このクライアントのアクセス VLAN ID を示します。

- [Status]：現在のクライアントのステータス。
  - [Idle]：正常の動作。クライアントのアソシエーション要求は拒否されていません。
  - [Auth Pending]：AAA トランザクションを実行しています。
  - [Authenticated]：802.11 認証が完了しています。
  - [Associated]：802.11 アソシエーションが完了しています。これは、現在クライアントがネットワークに接続されていることを示すために有線クライアントでも使用されます。
  - [Disassociated]：802.11 ディスアソシエーションが完了しています。これは、現在クライアントがネットワーク上に存在しないことを示すために有線クライアントでも使用されます。
  - [To Be Deleted]：ディスアソシエーション後にクライアントが削除されます。
  - [Excluded]：セキュリティの脅威と見なされたため、システムによって自動的に無効化されています。
- [Interface]：クライアントが接続するコントローラ インターフェイス（ワイヤレス）またはスイッチ インターフェイス（有線）。
- Protocol
  - [802.11]：ワイヤレス
  - [802.3]：有線
- [Association Time]：最後のアソシエーションの開始時間（ワイヤレス クライアントの場合）。有線クライアントの場合、これは、クライアントがスイッチ ポートに接続した時間です。クライアントがアソシエートされているが、ネットワーク上で問題がある場合は空欄になります。
- [CCX]：Lightweight ワイヤレスのみ。

ステップ 3　[Client and User] ページの MAC アドレスの横にあるオプション ボタンを選択して、アソシエートされたクライアント情報を表示します。次のようなさまざまなクライアント パラメータが表示されます。

- クライアント属性
- クライアント IPV6 アドレス
- クライアント統計情報

（注）　クライアントの統計には、クライアント詳細情報の後に統計情報が表示されます。

- クライアント アソシエーション履歴
- クライアント イベント情報
- クライアント ロケーション情報
- 有線ロケーション履歴
- クライアント CCX 情報

クライアント属性

[Clients and Users] リストからクライアントを選択すると、次のクライアント詳細情報が表示されます。クライアントは、MAC アドレスを使用して特定されます。

- 全般：次の情報がリストされます。
  - ユーザ名
  - IP アドレス
  - MAC アドレス

- ベンダー
- エンドポイント タイプ
- クライアント タイプ
- メディア タイプ
- モビリティ ロール
- ホスト名
- E2E
- 電力節約
- CCX
- ファンデーション サービス
- 管理サービス
- 音声サービス
- ロケーション サービス

（注）　ユーザ名の横にある アイコンをクリックすると、ユーザの関連するユーザにアクセスします。

- セッション：次のクライアント セッション情報をリストします。
  - コントローラ名
  - AP 名
  - AP IP アドレス
  - AP タイプ
  - AP ベース無線 MAC
  - アンカー アドレス
  - 802.11 ステート
  - アソシエーション ID
  - ポート
  - インターフェイス
  - SSID
  - プロファイル名
  - プロトコル
  - VLAN ID
  - AP モード
- セキュリティ（ワイヤレス クライアントおよびアイデンティティ有線クライアントのみ）：次のセキュリティ情報をリストします。
  - セキュリティ ポリシー タイプ
  - EAP タイプ
  - ネットワーク上
  - 802.11 認証

- 暗号化方式
- SNMP NAC の状態
- RADIUS NAC の状態
- AAA Override ACL 名
- AAA Override ACL の適用された状態
- リダイレクト URL
- ACL 名
- ACL の適用された状態
- FlexConnect ローカル認証
- Policy Manager ステート
- 認証 ISE
- 認可プロファイル名
- ポスチャ ステータス
- TrustSec セキュリティ グループ
- Windows AD ドメイン

（注） アイデンティティ クライアントは、認証タイプが 802.1x、MAC 認証バイパス、または Web 認証のクライアントです。アイデンティティ クライアント以外の認証タイプは N/A です。

（注） クライアント属性の下に表示されるデータは、アイデンティティ クライアントかそうでないかによって異なります。アイデンティティ クライアントの場合は、認証ステータス、監査セッション ID などのセキュリティ情報を確認できます。

- [Statistics]（ワイヤレスのみ）
- [Traffic]：クライアントのトラフィック情報を表示します。
- ワイヤレス クライアントの場合、クライアントのトラフィック情報はコントローラから取得します。有線クライアントの場合、クライアントのトラフィック情報は ISE から取得するため、スイッチ上でアカウンティング情報およびその他の必要な機能を有効にする必要があります。

Statistics

[Statistics] グループ ボックスには、選択したクライアントの次の情報が含まれます。

- クライアント AP アソシエーション履歴。
- クライアント RSSI 履歴（dBm）：クライアントがアソシエートされたアクセス ポイントで検出された RSSI（受信信号強度インジケータ）の履歴。
- クライアント SNR 履歴：クライアントがアソシエートされたアクセス ポイントで検出された SNR（クライアント RF セッションの信号対雑音比）の履歴。
- 送受信バイト（Kbps）：アソシエートされたアクセス ポイントで送受信したバイト数。
- 送受信パケット（毎秒）：アソシエートされたアクセス ポイントで送受信したパケット数。
- クライアントのデータ レート

この情報は、インタラクティブ グラフで表示されます。

クライアント IPV6 アドレス

[Client IPv6 Address] グループ ボックスには、選択したクライアントの次の情報が含まれます。

- IP アドレス：クライアント IPv6 アドレスを表示します。
- スコープ：グローバル固有、ローカル固有、およびリンク ローカルの 3 つのスコープ タイムがあります。
- アドレス タイプ：アドレス タイプを表示します。
- 検出時間：IP が検出された時間です。

アソシエーション履歴

[Association History] ダッシュレットには、選択したクライアントの過去 10 件のアソシエーション時間に関する情報が表示されます。この情報は、クライアントのトラブルシューティングの際に役立ちます。

[Association History] ダッシュレットには、次の情報が含まれます。

- アソシエーション時間
- 持続時間
- ユーザ名
- IP アドレス
- IP アドレス タイプ
- AP 名
- コントローラ名
- SSID

イベント

[Client Details] ページの [Event] グループ ボックスには、イベント タイプやイベントの日時など、このクライアントのすべてのイベントが表示されます。

- イベント タイプ
- イベント時間
- 説明

マップ

[View Location History] をクリックすると、有線クライアントおよびワイヤレス クライアントのロケーション履歴の詳細が表示されます。

有線クライアントまたはワイヤレス クライアントの次のロケーション履歴情報が表示されます。

- タイムスタンプ
- 状態
- ポート タイプ
- スロット
- モジュール
- ポート
- ユーザ名

- IP アドレス
- スイッチ IP
- サーバ名
- マップ位置の都市ロケーション

ビルディングの設定

キャンパス マップをデータベースに追加したことがあるかどうかに関係なく、ビルディングを NCS データベースに追加できます。ここでは、ビルディングをキャンパス マップに追加する方法、または独立したビルディング（キャンパスの一部ではないビルディング）を NCS データベースに追加する方法を説明します。

この項では、次のトピックを扱います。

キャンパス マップへのビルディングの追加

NCS データベース内のキャンパス マップにビルディングを追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2　目的のキャンパスをクリックします。[Site Maps] > [Campus Name] ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 4　[Campus Name] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

a. ビルディング名を入力します。

b. ビルディング問い合わせ先の名前を入力します。

c. 地上のフロア数と地下のフロア数を入力します。

d. 水平位置（ビルディングの四角形の隅からキャンパス マップの左端までの距離）と垂直位置（ビルディングの四角形の隅からキャンパス マップの上端までの距離）をフィート単位で入力します。

（注）　測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

e. ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注）　水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

ヒント Ctrl キーを押した状態でクリックすることで、キャンパス マップの左上隅にある境界領域のサイズを変更できます。境界領域のサイズを変更すると、ビルディングの水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。

f. [Place] をクリックして、ビルディングをキャンパス マップ上に配置します。NCS では、キャンパス マップのサイズに合わせてサイズ変更されたビルディングの四角形が作成されます。

g. ビルディングの四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。

（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

h. [Save] をクリックして、このビルディングとキャンパス上の位置をデータベースに保存します。NCS では、キャンパス マップ上にあるビルディングの四角形の中にビルディング名が保存されます。

（注） ビルディングには、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 5　（任意）新しい屋外領域に位置プレゼンス情報を割り当てる手順は、次のとおりです。

a. [Select a command] ドロップダウン リストから、[Edit Location Presence Info] を選択します。[Go] をクリックします。[Location Presence] ページが表示されます。

（注） デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。キャンパス マップにビルディングを追加する際は、キャンパスのロケーション情報をインポートできます。
チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。
1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

b. [Civic Address] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

c. デフォルトでは、[Override Child's Presence Information] チェックボックスはオンになっています。独立したビルディングについては、この設定を変更する必要はありません。

ステップ 6　[Save] をクリックします。

独立したビルディングの追加

NCS データベースに独立したビルディングを追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2　[Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 3　[Maps] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

a. ビルディング名を入力します。

b. ビルディング問い合わせ先の名前を入力します。

（注）　新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

c. 地上のフロア数と地下のフロア数を入力します。

d. ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注）　測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

（注）　水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

e. [OK] をクリックして、このビルディングをデータベースに保存します。

ステップ 4　（任意）新しいビルディングに位置プレゼンス情報を割り当てる手順は、次のとおりです。

a. [Select a command] ドロップダウン リストから、[Location Presence] を選択します。[Go] をクリックします。[Location Presence] ページが表示されます。

b. [Civic] タブ、[GPS Markers] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [GPS Markers] では、経度と緯度でキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注）　選択した各パラメータには、上記のすべてが含まれています。たとえば、[Advanced] を選択した場合、ユーザからの要求により GPS および Civic 位置情報も提供されます。選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

（注）　クライアントが、キャンパスに対して GPS Markers パラメータで設定されていないビルディング、フロア、または屋外領域などの位置情報を要求した場合、エラー メッセージが返されます。

c. デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。キャンパス マップにビルディングを追加する際は、ロケーション情報をインポートできます。チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

ステップ 5　[Save] をクリックします。

（注）　独立したビルディングは、システム キャンパス内に自動的に配置されます。

ビルディングの表示

現在のビルディング マップを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　ビルディング マップの名前をクリックして、詳細ページを開きます。[Building View] ページには、各フロアのフロア マップの一覧とマップの詳細が表示されます。

（注）　[Building View] ページの [Floor] 列見出しをクリックして、一覧をフロアの昇順または降順にソートできます。

マップの詳細には、次の情報が含まれます。

- フロア領域
- フロア インデックス：フロア レベルを示します。マイナスの数は地下のフロア レベルを示します。
- 連絡先
- ステータス：このマップ上に配置されているアクセス ポイントまたは子のアクセス ポイントで、重大度の最も高いアラームを示します。
- マップに配置されているアクセス ポイントの総数。
- マップに配置されている 802.11a/n 無線および 802.11b/g/n 無線の数。
- 停止している（OOS）無線の数。
- クライアント数：数字のリンクをクリックすると、[Monitor] > [Clients] ページが表示されます。詳細については、「Monitoring Clients and Users」（P.10-10）を参照してください。

ステップ 3　[Select a command] ドロップダウン リストには、次のオプションが表示されます。

- [New Floor Area]：詳細については、「キャンパス マップへのビルディングの追加」（P.9-23）を参照してください。
- [Edit Building]：詳細については、「ビルディングの編集」（P.9-27）を参照してください。
- [Delete Building]：詳細については、「ビルディングの削除」（P.9-27）を参照してください。

ビルディングの編集

現在のビルディング マップを編集するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　ビルディング マップの名前をクリックして、詳細ページを開きます。

ステップ 3　[Select a command] ドロップダウン リストから [Edit Building] を選択します。

ステップ 4　[Building Name]、[Contact]、[Number of Floors]、[Number of Basements]、および [Dimensions (feet)] に必要な変更を加えます。

（注）　測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

ステップ 5　[OK] をクリックします。

ビルディングの削除

現在のビルディング マップを削除するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　削除するビルディングのチェックボックスをオンにします。

ステップ 3　マップ リスト下部の [Delete] をクリックします（または、[Select a command] ドロップダウン リストから [Delete Maps] を選択して、[Go] をクリックします）。

ステップ 4　[OK] をクリックして、削除を実行します。

（注）　ビルディングを削除すると、そのコンテナ マップもすべて削除されます。削除されるすべてのマップのアクセス ポイントが、未割り当てステートに移行されます。

ビルディングの移動

別のキャンパスにビルディングを移動するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するビルディングのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Move Buildings] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　ドロップダウン リストから対象のキャンパスを選択します。

ステップ 6　移動するビルディングを選択します。現在のロケーションを維持するビルディングをオフにします。

ステップ 7　[OK] をクリックします。

Geo-Location のモニタリング

MSE は、有線クライアント、有線エンド ポイント、スイッチ、コントローラ、ワイヤレス ネットワーク構成内にあるアクセス ポイントの物理ロケーションを提供します。現在、MSE はノースバウンド エンティティからサウスバウンド エンティティまでの外部エンティティに Geo-Location 形式でロケーション情報を提供しています。

MSE によって提供される Geo-Location 情報の精度を向上するために、この機能はデバイスのジオメトリック ロケーション座標を Geo-Location 座標（経度と緯度）に変換し、ノースバウンド インターフェイスとサウスバウンド インターフェイスを介して外部エンティティに提供します。

（注）　Geo-Location の計算には、少なくとも 3 つの GPS マーカーが必要です。追加できる GPS マーカーの最大数は 20 です。

この項では、次のトピックを扱います。

- 「フロア マップへの GPS マーカーの追加」（P.9-28）
- 「GPS マーカーの編集」（P.9-29）
- 「フロアにある GPS マーカーの削除」（P.9-29）

フロア マップへの GPS マーカーの追加

GPS マーカーをフロア マップに追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2　[Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3　左上のメニューの [Add/Edit GPS Markers Information] メニュー オプションをクリックして、[Add/Edit GPS] ページを表示します。

マップの左上隅（X = 0、Y = 0）に [GPS Marker] アイコンが表示されます。

ステップ 4　[GPS Marker] アイコンをドラッグして、マップ上の希望する場所に配置することができます。また、左側のサイドバー メニューにある [GPS Marker Details] テーブルに X と Y の位置の値を入力して、マーカーを希望する位置に移動することができます。

（注）　追加したマーカーの位置が近すぎると、Geo-Location 情報の精度は低下します。

ステップ 5　左側のサイドバー メニューで選択した [GPS Marker] アイコンの経度と緯度を入力します。

ステップ 6　[Save] をクリックします。

[GPS Marker] の情報がデータベースに保存されます。

ステップ 7　[Apply to other Floors of Building] をクリックして、ビルディングの 1 フロアの GPS マーカーをそのビルディングの残りのすべてのフロアにコピーします。

GPS マーカーの編集

フロアにある GPS マーカーを編集するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2　[Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3　左上のメニューの [Add/Edit GPS Markers Information] メニュー オプションをクリックして、[Add/Edit GPS] ページを表示します。

ステップ 4　フロアにある既存の GPS マーカーを選択します。

ステップ 5　左側のサイドバー メニューから、その GPS マーカーにアソシエートされている [Latitude]、[Longitude]、[X Position]、および [Y Position] を変更できます。

ステップ 6　[Save] をクリックします。

これで、変更した GPS マーカーの情報がデータベースに保存されます。

フロアにある GPS マーカーの削除

フロアにある GPS マーカーを削除するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2　[Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3　左上のメニューの [Add/Edit GPS Markers Information] メニュー オプションをクリックして、[Add/Edit GPS] ページを表示します。

ステップ 4　左側のサイドバー メニューから、フロアにある既存の GPS マーカーを選択します。

（注）　複数の [GPS Markers] チェックボックスをオンにすることで、フロアにある複数の GPS マーカーを削除できます。

ステップ 5　[Delete GPS Marker] をクリックします。

選択した GPS マーカーがデータベースから削除されます。

CHAPTER 10

MSAP

Cisco Mobility Services Advertisement Protocol（MSAP）では、MSAP クライアントおよびサーバの要件を規定し、それらの間でのメッセージ交換を記述します。モバイル デバイスは、MSAP を使用して MSAP サーバから Wi-Fi インフラストラクチャを介してサービス アドバタイズメントを取得できます。このリリースのモビリティ サービス エンジン（MSE）では、MSAP が導入され、サーバ機能が提供されています。

MSAP は、ネットワーク接続を確立するためのポリシー セットを使用して設定されたモバイルデバイスで使用します。MSAP により、モバイル デバイスは、ローカル ネットワークで使用可能なネットワークベース サービスまたはサービス プロバイダーを介して有効にされたサービスを検出しやすくなります。MSAP は、モバイル デバイスで使用可能なサービスが記述されるサービス アドバタイズメントを提供します。モバイルデバイスは、サービス アドバタイズメントを受信すると、そのアイコンとデータがモバイル デバイスのユーザ インターフェイスに表示されます。表示されたアイコンをクリックして、アドバタイズされたサービスを起動できます。

この章は、次の内容で構成されています。

MSAP のライセンス

MSAP ライセンスは、MSE によってサポートされるサービス アドバタイズメントの数に基づきます。MSAP に使用できる評価ライセンスは 1 つだけあり、サービス アドバタイズメント クリックが 1000 に制限されています。

MSAP サービス アドバタイズメントのプロビジョニング

新しい MSAP アドバタイズメントを追加するには、次の手順を実行します。

ステップ 1　[Services] > [MSAP] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Service Advertisements] を選択し、[Go] をクリックします。

[Service Advertisement Details] ページが表示されます。

ステップ 3　[Provider Name] テキスト ボックスにサービス プロバイダーの名前を入力します。これは、クライアントにアドバタイズメントを提供するプロバイダーの名前です。

ステップ 4　[Choose File] をクリックして、サービス プロバイダーに関連付けるアイコンを選択します。これは、クライアント ハンドセットに表示されるアイコンです。

サービス アドバタイズメントへの場所のポリシーの追加

（注）　[Services] > [MASP] を選択して、サービス アドバタイズメントを場所にも適用できます。サービス アドバタイズメントの適用方法については、「場所へのサービス アドバタイズメントの適用」（P.10-3）を参照してください。

ステップ 5　[Add Venue] をクリックして、アドバタイズメントをブロードキャストする場所を指定します。

[Add/Edit Venue] ページが表示されます。

ステップ 6　[Venue Name] テキスト ボックスに場所の名前を入力します。

ステップ 7　[Area Type] ドロップダウン リストから、サービス アドバタイズメントを表示するエリア タイプを選択します。指定できる値は、[Floor Area] および [Outdoor area] です。

ステップ 8　[Campus] ドロップダウン リストから、サービス アドバタイズメントを表示させるキャンパス名を選択します。

ステップ 9　[Building] ドロップダウン リストから、アドバタイズメントを表示させるビルディング名を選択します。

ステップ 10　[Floor] ドロップダウン リストから、フロア タイプを選択します。

（注）　選択するフロアによって、[Display near selected APs] の情報が変わります。

ステップ 11　[SSID] ドロップダウン リストから、サービス アドバタイズメントをブロードキャストさせる SSID を選択します。複数の SSID を選択できます。

ステップ 12　[Display Rule] オプション ボタンを選択します。[Display everywhere] または [Display near selected APs] オプション ボタンのいずれかを選択できます。デフォルトでは、[Display everywhere] が選択されています。

[Display everywhere] を選択した場合、これらの SSID を提供するすべての MSAP 対応コントローラを検索し、そのコントローラを MSE に割り当てます。

[Display near selected APs] を選択した場合、次のパラメータを設定できます。

- [AP] : アドバタイズメントをブロードキャストする AP を選択します。
- [Radio] : アドバタイズメントをブロードキャストする無線周波数を選択します。選択した無線帯域の近くにモバイルデバイスがある場合、サービス アドバタイズメントが表示されます。指定できる値は 2.4 GHz または 5 GHz です。
- [min RSSI] : ユーザ インターフェイスにサービス アドバタイズメントを表示する RSSI の値を入力します。

ステップ 13　[Save] をクリックして、場所を追加します。[Service Advertisement Details] ページの場所のリストに、場所が追加されます。

サービス アドバタイズメントへのサービス要約情報の追加

ステップ 14　[Add Advertisement] をクリックします。

[Add/Edit Advertisement] ページが表示されます。

ステップ 15　[Advertisement Type] ドロップダウン リストから、表示するアドバタイズメントのタイプを選択します。

ステップ 16　[Friendly Name] テキスト ボックスに、ハンドセットに表示する名前を入力します。

ステップ 17　[Friendly Description] テキスト ボックスにサービスの説明を入力します。

ステップ 18　ハンドセットの各タイプの URL を入力します。URL は、サービスを取得できるロケーションを特定します。[Add More URL] をクリックして、複数の URL を追加できます。

ステップ 19　[Save] をクリックします。この情報は MSE に適用され、自動的に同期されます。

サービス アドバタイズメントの削除

サービス アドバタイズメントを削除するには、次の手順を実行します。

ステップ 1　[Services] > [MSAP] を選択します。

[MSAP] ページが表示されます。

ステップ 2　削除するサービス アドバタイズメントのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Delete Service Advertisement] を選択し、[Go] をクリックするか、[MSAP] ページの [Delete] をクリックします。

ステップ 4　[OK] をクリックして、削除を実行します。

場所へのサービス アドバタイズメントの適用

サービス アドバタイズメントを場所に適用するには、次の手順を実行します。

ステップ 1　[Services] > [MSAP] を選択します。

ステップ 2　場所に適用するサービス アドバタイズメントのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Apply to Venue(s)] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　「MSAP サービス アドバタイズメントのプロビジョニング」(P.10-1) のステップ 6 からステップ 13 を実行します。

または

[MSAP] ページで [Apply to Venues] をクリックして、「MSAP サービス アドバタイズメントのプロビジョニング」（P.10-1）のステップ 6 からステップ 13 を実行します。

MSE ごとの設定済みサービス アドバタイズメントの表示

MSE ごとに設定済みのサービス アドバタイズメントを表示するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engine] の順に選択します。

ステップ 2　[Device Name] をクリックして、そのプロパティを表示します。

[General Properties] ページが表示されます。

ステップ 3　左側のサイドバーのメニューから、[MSAP Service] > [Advertisements] の順に選択します。

[MSAP Service] ページに次の情報が表示されます。

- [Icon]：サービス プロバイダーに関連付けられたアイコンを表示します。
- [Provide Name]：サービス プロバイダー名を表示します。
- [Venue Name]：場所の名前を表示します。
- Advertisements
  - [Friendly Name]：ハンドセットに表示されるわかりやすい名前。
  - [Advertisement Type]：ハンドセットに表示されるアドバタイズメントのタイプ。

MSAP 統計の表示

MSAP 統計を表示するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engine] の順に選択します。

ステップ 2　[Device Name] をクリックして、そのプロパティを表示します。

[General Properties] ページが表示されます。

ステップ 3　左側のサイドバーのメニューから、[MSAP Service] > [Statistics] の順に選択します。

[MSAP Service] ページに次の情報が表示されます。

- [Top 5 Active Mobile MAC addresses]：特定の場所で最もアクティブなモバイルについての情報を表示します。
- [Top 5 Service URIs]：特定の場所またはプロバイダー上でサービスの使用量についての情報を表示します。

MSAP ライセンス情報の [MSE Summary] ページの表示

MSE ライセンスの詳細については、「Managing Mobility Services Engine (MSE) Licenses」（P.15-140）を参照してください。

サービス アドバタイズメントの同期ステータスの表示

サービス アドバタイズメントの同期ステータスを表示するには、次の手順を実行します。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Service Advertisements] を選択します。[Service Advertisements] ページに次の情報が表示されます。

- [Provider Name]：サービス プロバイダーの名前を表示します。
- [Service]：特定のアドバタイズメントが使用しているサービスのタイプを表示します。
- [MSE]：サービス アドバタイズメントが MSE と同期しているかどうかを表示します。
- [Sync Status]：同期ステータスを表示します。緑の 2 つの矢印アイコンは、その対応する要素が、MSE などの指定されたサーバと同期していることを示します。灰色の 2 つの矢印と赤い円のアイコンは、対応する項目が指定のサーバと同期していないことを示します。
- [Message]：アドバタイズメントの同期の失敗に関連するメッセージがあれば表示します。

MSAP レポート

ここでは、MSAP レポートの作成方法について説明します。内容は次のとおりです。

- 「Mobile MAC Statistics」（P.10-5）
- 「Service URI Statistics」（P.10-6）

Mobile MAC Statistics

Report Launch Pad の [Mobile MAC Statistics] をクリックして [Mobile MAC Statistics Reports] ページを開きます。このページで、現在保存されているレポート テンプレートを有効、無効、削除、または実行できます。

レポートを新規作成するには、[Report Launch Pad] ページまたは [Mobile MAC Statistics Reports] ページで [New] をクリックします。詳細については、「Mobile MAC Statistics レポートの設定」（P.10-5）を参照してください。

Mobile MAC Statistics レポートの設定

ここでは、Mobile MAC Statistics レポートの設定方法について説明します。

設定

- [Report Title]：このレポート テンプレートを保存する場合は、レポート名を入力します。
- Report by
  - [Mobile MAC by MSAP Server]：MSAP サーバに基づいてモバイル MAC のレポートを生成する場合に、このオプションを選択します。
  - [Mobile MAC by Venue]：場所に基づいてモバイル MAC のレポートを生成する場合に、このオプションを選択します。
- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注）　[Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Reporting Period
  - [Last] : [Last] オプション ボタンを選択し、ドロップダウン リストから期間を選択します。
  - [From] : [From] オプション ボタンを選択して、開始日時と終了日時を入力します。テキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして日付を選択できます。ドロップダウン リストから時間と分を選択します。

（注）　レポート期間は、アラームの最終検出時刻に基づいています。時間は UTC タイム ゾーンです。

（注）　固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Mobile MAC Statistics レポートの結果には、次の情報が含まれています。

- モバイル MAC
- クリック数

（注）　このレポートには、MSE や場所別に、クリック数に基づく最もアクティブなモバイル MAC が示されます。複数の MSE を選択した場合は、選択したソート順序によって、MSE ごとに上位のモバイル MAC がグループ化されます。

Service URI Statistics

[Report Launch Pad] ページの [Service URI Statistics] をクリックして [Service URI Statistics Reports] ページを開きます。このページで、現在保存されているレポート テンプレートを有効、無効、削除、または実行できます。

レポートを新規作成するには、[Report Launch Pad] または [Mobile MAC Statistics Reports] ページで [New] をクリックします。詳細については、「Service URI Statistics レポートの設定」（P.10-6）を参照してください。

Service URI Statistics レポートの設定

ここでは、Service URI Statistics レポートの設定方法について説明します。

設定

- [Report Title] : このレポート テンプレートを保存する場合は、レポート名を入力します。
- Report by
  - [Service URI by MSAP Server] : MSAP サーバに基づいてモバイル MAC のレポートを生成する場合に、このオプションを選択します。
  - [Service URI by Venue] : 場所に基づいてサービス URI のレポートを生成する場合に、このオプションを選択します。

  - [Service URI by Mobile MAC] : モバイル MAC に基づいてサービス URI のレポートを生成する場合に、このオプションを選択します。
  - [Service URI by Provider] : プロバイダーに基づいてサービス URI のレポートを生成する場合に、このオプションを選択します。
- [Report Criteria] : レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

  （注）　[Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Reporting Period
  - [Last] : [Last] オプション ボタンを選択し、ドロップダウン リストから期間を選択します。
  - [From] : [From] オプション ボタンを選択して、開始日時と終了日時を入力します。テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。ドロップダウン リストから時間と分を選択します。

  （注）　レポート期間は、アラームの最終検出時刻に基づいています。時間は UTC タイム ゾーンです。

（注）　固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Service URI Statistics レポートの結果には、次の情報が含まれています。

- サービス URI
- モバイル MAC
- クリック数
- このレポートには、MSE や場所別に、クリック数に基づいて上位のサービス URI が示されます。複数の MSE を選択した場合は、選択したソート順序によって、MSE ごとに上位のサービス URI がグループ化されます。

CHAPTER 11

メンテナンス操作の実行

この章では、モビリティ サービス エンジン データのバックアップおよび復元方法とモビリティ サービス エンジン ソフトウェアの更新方法について説明します。また、その他のメンテナンス操作についても説明します。

この章は、次の内容で構成されています。

ガイドラインと制限事項

- パスワードを忘れないようにしてください。パスワードの変更は絶対に必要な場合にだけ行ってください。
- 紛失したルート パスワードを回復する際、単一ユーザ モード パスワードを設定する場合はシェル プロンプトは表示されません。

失われたパスワードの復旧

モビリティ サービス エンジンのパスワードを紛失または忘れた場合に回復するには、次の手順に従います。

ステップ 1 [GRUB] ページが表示されたら、Esc を押してブート メニューに入ります。

ステップ 2 e を押して編集します。

ステップ 3 kernel で始まる行に移動し、e を押します。

行の最後に、スペースに続けて数字の **1** を入力します。Enter を押してこの変更を保存します。

ステップ 4 b を押してブートを開始します。

ブート シーケンスの最後にシェル プロンプトが表示されます。

ステップ 5　**passwd** コマンドを入力すると、ルート パスワードを変更できます。

ステップ 6　新しいパスワードを入力して確定します。

ステップ 7　マシンを再起動します。

失われたルート パスワードの回復

モビリティ サービス エンジンのルート パスワードを紛失または忘れた場合に回復するには、次の手順に従います。

ステップ 1　[GRUB] ページが表示されたら、Esc を押してブート メニューに入ります。

ステップ 2　e を押して編集します。

ステップ 3　kernel で始まる行に移動し、e を押します。

行の最後に、スペースに続けて数字の **1** を入力します。Enter を押してこの変更を保存します。

ステップ 4　b を押してブート シーケンスを開始します。

ブート シーケンスの最後にシェル プロンプトが表示されます。

（注）　単一ユーザ モードパスワードを設定する場合は、シェル プロンプトは表示されません。

ステップ 5　**passwd** コマンドを入力すると、ルート パスワードを変更できます。

ステップ 6　新しいパスワードを入力して確定します。

ステップ 7　マシンを再起動します。

（注）　ルート パスワードを忘れないようにしてください。パスワードの変更は絶対に必要な場合にだけ行ってください。

モビリティ サービス エンジン データのバックアップおよび復元

ここでは、モビリティ サービス エンジン データのバックアップおよび復元方法について説明します。また、自動バックアップを有効にする方法についても説明します。

この項では、次のトピックを扱います。

ガイドラインと制限事項

- バックアップは、NCS のインストール時に指定した FTP ディレクトリに保管されます。
- 他の NCS ページで他のモビリティ サービス エンジン操作を実行しながら、バックアップ プロセスをバックグラウンドで実行できます。

モビリティ サービス エンジンの履歴データのバックアップ

NCS には、モビリティ サービス エンジン データをバックアップする機能があります。

モビリティ サービス エンジン データをバックアップするには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　バックアップするモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Maintenance] の順に選択します。

ステップ 4　[Backup] をクリックします。

ステップ 5　バックアップの名前を入力します。

ステップ 6　[Submit] をクリックし、NCS が実行されているサーバのハード ドライブに履歴データをバックアップします。

バックアップの処理中に、バックアップのステータスをこのページに表示できます。バックアップ プロセス中に、このページには 3 つの項目が表示されます。（1）[Last Status] テキスト ボックスには、バックアップのステータスを示すメッセージが表示され、（2）[Progress] テキスト ボックスには、バックアップの完了率が表示され、（3）[Started at] テキスト ボックスには、バックアップの開始日時が表示されます。

（注）　他の NCS ページで他のモビリティ サービス エンジン操作を実行しながら、バックアップ プロセスをバックグラウンドで実行できます。

（注）　バックアップは、NCS のインストール時に指定した FTP ディレクトリに保管されます。

モビリティ サービス エンジンの履歴データの復元

（バックアップからの）履歴データに NCS を使用できます。

モビリティ サービス エンジン データを復元するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　復元するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Maintenance] の順に選択します。

ステップ 4　[Restore] をクリックします。

ステップ 5　ドロップダウン リストから、復元するファイルを選択します。

ステップ 6　モビリティ サービス エンジンからすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。

このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 7　[Submit] をクリックして復元プロセスを開始します。

ステップ 8　[OK] をクリックし、Cisco NCS Server のハード ドライブからデータを復元することを確定します。

復元が完了すると、NCS にそのことを示すメッセージが表示されます。

（注）　復元プロセスの実行中に、他のモビリティ サービス エンジン操作を実行しないでください。

ロケーション データの自動バックアップの有効化

ロケーション データの自動バックアップを定期的に実行するように NCS を設定できます。

モビリティ サービス エンジンのロケーション データの自動バックアップを有効にするには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　[Mobility Service Backup] チェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

バックアップは、NCS のインストール時に指定した FTP ディレクトリに保管されます。

モビリティ サービス エンジンへのソフトウェアのダウンロード

ソフトウェアをモビリティ サービス エンジンにダウンロードするには、次の手順に従います。

ステップ 1　アプリケーション コードのダウンロードに使用する Cisco NCS Server または外部 FTP サーバから、モビリティ サービス エンジンに対して ping を実行できることを確認します。

ステップ 2　[Services] > [Mobility Services Engine] の順に選択します。

ステップ 3　ソフトウェアをダウンロードするモビリティ サービス エンジンの名前をクリックします。

ステップ 4　左側のサイドバーのメニューから、[System] > [Maintenance] > [Download Software] の順に選択します。

ステップ 5　ソフトウェアをダウンロードするには、次のいずれかを実行します。

- NCS ディレクトリにリストされているソフトウェアをダウンロードするには、[Select from uploaded images to transfer into the Server] オプション ボタンを選択します。ドロップダウン リストからバイナリ イメージを選択します。

  NCS により、バイナリ イメージが NCS のインストール時に指定した FTP サーバ ディレクトリにダウンロードされます。

- ローカルまたはネットワーク経由で使用可能なダウンロード済みソフトウェアを使用するには、[Browse a new software image to transfer into the Server] オプション ボタンを選択し、[Choose File] をクリックします。ファイルを見つけ、[Open] をクリックします。

ステップ 6　[Download] をクリックし、ソフトウェアをモビリティ サービス エンジンの /opt/installers ディレクトリにダウンロードします。

ステップ 7　イメージがモビリティ サービス エンジンに転送されたら、モビリティ サービス エンジンのコマンドライン インターフェイスにログインします。

ステップ 8　**./.bin mse image** コマンドを入力して、/opt/installers ディレクトリからインストーラ イメージを実行します。これによりソフトウェアがインストールされます。

ステップ 9　ソフトウェアを実行するには、**/etc/init.d/msed start** コマンドを入力します。

（注）　ソフトウェアを停止するには、**/etc/init.d/msed stop** コマンドを入力し、ステータスをチェックするには、**/etc/init.d/msed status** コマンドを入力します。

ソフトウェアの手動ダウンロード

NCS を使用してモビリティ サービス エンジン ソフトウェアを自動的に更新しない場合、次の手順に従い、ローカル（コンソール）またはリモート（SSH）接続を使用してソフトウェアを手動でアップグレードします。

ステップ 1　新しいモビリティ サービス エンジン イメージをハード ドライブに転送します。

a.　root としてログインし、バイナリ設定を使用して外部 FTP サーバのルート ディレクトリからイメージを送信します。リリース ノート形式は CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz のようになり、リリースごとに変更されます。

（注）　この時点では、モビリティ サービス エンジン イメージは圧縮されています。

（注）　FTP サーバのデフォルト ログイン名は ftp-user です。

入力は、次の例のようになります。

```
# cd /opt/installers
# ftp <FTP Server IP address>
Name: <login>
Password: <password>
binary
get CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz
<CTRL-Z>
#
```

b.　イメージ（CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz）がモビリティ サービス エンジンの /opt/installers ディレクトリにあることを確認します。

c.　イメージ ファイルを圧縮解除（解凍）するには、次のコマンドを入力します。

gunzip CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz

圧縮解除すると、bin ファイルが生成されます。

d. CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz ファイルにルート ユーザの実行権限があることを確認します。ない場合は、次のコマンドを入力します。

```
chmod 755 CISCO-MSE-L-K9-x-x-x-x.bin.
```

ステップ 2　モビリティ サービス エンジンを手動で停止します。

ステップ 3　root としてログインし、次のコマンドを入力します。

```
/etc/init.d/msed stop.
```

ステップ 4　新しいモビリティ サービス エンジン イメージをインストールするには、次のコマンドを入力します。

```
/opt/installers/CISCO-MSE-L-K9-x-x-x-x.bin.
```

ステップ 5　次のコマンドを入力して、新しいモビリティ サービス エンジン ソフトウェアを開始します。

```
/etc/init.d/msed start
```

注意　スクリプト ファイルをアンインストールする次の手順を実行するように指示された場合に限り、この手順を実行します。ファイルを削除すると、履歴データが不必要に消去されます。

ステップ 6　次のコマンドを入力して、モビリティ サービス エンジンのスクリプト ファイルをアンインストールします。

```
/opt/mse/uninstall
```

NTP サーバの設定

NTP サーバを設定して、モビリティ サービス エンジンの時刻と日付を設定できます。

（注）

- モビリティ サービス エンジンの自動インストール スクリプトの一環として、NTP をイネーブルにし、NTP サーバ IP アドレスを入力するように求めるプロンプトが自動的に表示されます。自動インストール スクリプトの詳細については、次の URL にある『*Cisco 3350 Mobility Services Engine Getting Started Guide*』または『*Cisco 3310 Mobility Services Engine Getting Started Guide*』を参照してください。

  http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

- モビリティ サービス エンジンのインストール後に NTP サーバのインストールを追加または変更する必要がある場合、自動インストール スクリプトを再実行します。スクリプトをタブで指定して他の値を調整せずに NTP サーバを設定できます。

（注）　NTP サーバの設定の詳細については、Linux の設定ガイドを参照してください。

システムのリセット

モビリティ サービス エンジン ハードウェアの再起動またはシャットダウンについては、「システムの再起動またはシャットダウン」（P.6-10）を参照してください。

コンフィギュレーション ファイルの消去

コンフィギュレーション ファイルの消去については、「システム データベースの消去」（P.6-10）を参照してください。

APPENDIX A

wIPS ポリシー アラーム リファレンス

この付録では、wIPS が対応している脅威のタイプの概要について説明します。構成は次のとおりです。

セキュリティ IDS/IPS の概要

企業環境に WLAN を追加すると、ネットワーク セキュリティに対する新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無認可のユーザに公開する可能性があります。個人の使用のために従業員によって設置された不正アクセス ポイントは通常、企業のセキュリティ ポリシーに準拠していません。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正アクセス ポイントの脅威以外にも、アクセス ポイントの設定ミスや未設定、DoS（サービス拒否）攻撃といったさまざまなワイヤレス セキュリティ リスクや侵入の可能性が存在します。

Cisco Adaptive Wireless IPS（wIPS）は適切なセキュリティ設定を検証し、侵入攻撃の可能性を検出することで、セキュリティの脅威への対処を支援します。wIPS は、包括的なセキュリティ モニタリング テクノロジー スイートを使用して、次のカテゴリ内の 100 件を超えるさまざまな脅威状況をユーザに警告します。

- ユーザ認証とトラフィック暗号化
- 不正デバイスとアドホック モード デバイス
- 設定の脆弱性
- 侵入検知（セキュリティ突破）
- 侵入検知（DoS 攻撃）

wIPS の機能を最大限に活用するために、セキュリティ導入ポリシーに最も適したものになるようにセキュリティ アラームをカスタマイズできます。たとえば WLAN の導入時に特定ベンダーのアクセス ポイントを導入する場合、そのアクセス ポイントまたはセンサーによって別のベンダーのアクセス ポイントが検出されると不正アクセス ポイント アラームを生成するように製品をカスタマイズできます。

さまざまな WLAN 環境用の設定済みのプロファイル

インストール中に、実装されている WLAN ネットワークに基づいて適切なプロファイルをユーザが選択できます。

wIPS は、次の項目に個別のプロファイルを提供します。

- Enterprise best practice
- Enterprise rogue detection only
- Financial（Gramm-Leach-Bliley 法に準拠）
- HealthCare（Health Insurance Portability and Accountability 法に準拠）
- Hotspot implementing 802.1x security
- Hotspot implementing NO security
- Tradeshow environment
- Warehouse/manufacturing environment
- Government/Military（8100.2 指令に準拠）
- Retail environment

適切なプロファイルを選択すると、wIPS は、該当 WLAN 環境に適したポリシー プロファイルのアラームを有効または無効にします。たとえば、医療機関の場合、[Helthcare] プロファイルを選択すると HIPAA 準拠のために必要なすべてのアラームが有効になります。管理者はインストール後にアラームを有効または無効にしたり、プリファレンスごとに閾値を変更したりできます。

wIPS システムは、IDS（侵入検知システム）であるだけではなく、IPS（侵入防御システム）でもあります。

Cisco Adaptive Wireless IPS のポリシーは、「wIPS：DoS（サービス拒否）攻撃」と「wIPS：セキュリティ突破」という 2 つのセキュリティ サブカテゴリに分類されます。

この項では、次のトピックを扱います。

- 「侵入検知：DoS 攻撃」（P.A-2）
- 「侵入検知：セキュリティ突破」（P.A-24）

侵入検知：DoS 攻撃

ワイヤレス DoS（サービス拒否）攻撃は、レイヤ 1 またはレイヤ 2 における WLAN のさまざまな脆弱性を悪用してワイヤレス サービスを妨害することを狙いとしています。DoS 攻撃は、物理的な RF 環境、アクセス ポイント、クライアント ステーション、またはバックエンド認証 RADIUS サーバをターゲットとする可能性があります。たとえば、オフィスがある建物の外部から、高出力指向性アンテナを使用した遠隔 RF 電波妨害攻撃が行われることがあります。侵入者が使用する攻撃ツールは、スプーフされた 802.11 管理フレームやスプーフされた 802.1x 認証フレームなどのハッキング技法、または単に総当たりのパケット フラッディング方法を利用します。

このような攻撃の中には、ワイヤレスの特性とワイヤレス プロトコル標準を対象にするものがあります。このため、シスコは、このような攻撃の多くを未然に防ぐため、802.11i のベースとなる管理フレーム保護を開発しました。（MFP の詳細については、Cisco NCS オンライン ヘルプを参照してください）。wIPS は、攻撃シグニチャの照合が行われる早期検知システムによってこのソリューションに寄与しています。wIPS の DoS 検出機能は WLAN レイヤ 1（物理層）とレイヤ 2（データ リンク層、802.11、802.1x）を対象にしています。強力な WLAN 認証および暗号化メカニズムが採用されている場合、上位層（IP 層以上）への DoS 攻撃が困難になります。wIPS サーバでは強力な認証および暗号化ポリシーを検証することで、WLAN 防衛が強化されます。さらに、Dos 攻撃およびセキュリティ突破に対する wIPS の侵入検知は、潜在的なワイヤレス攻撃に対する毎日 24 時間年中無休の完璧なモニタリングを提供します。

この項では、DoS 攻撃の 3 つのサブカテゴリについて説明します。この項は次のトピックで構成されています。

- 「アクセス ポイントに対する DoS 攻撃」（P.A-3）

アクセス ポイントに対する DoS 攻撃

アクセス ポイントに対する DoS 攻撃は主に次の事項を前提として実行されます。

- アクセス ポイントのリソースが限られている。（クライアントごとのアソシエーション ステート テーブルなど）。
- WLAN 管理フレームおよび認証プロトコル 802.11 と 802.1x に暗号化メカニズムがない。

ワイヤレス侵入者は、スプーフした MAC アドレスを使って多数のワイヤレス クライアントをエミュレートし、アクセス ポイントのリソース（最も重要なものとしてクライアント アソシエーション テーブル）を枯渇させます。エミュレートされた各クライアントはターゲット アクセス ポイントとのアソシエートと認証を試行しますが、プロトコル トランザクションは未完了のままになります。アクセス ポイント リソースとクライアント アソシエーション テーブルがこのようなエミュレートされたクライアントとその未完了認証ステートでいっぱいになるため、攻撃を受けたアクセス ポイントは正規のクライアントに対処できなくなります。このようにして DoS 攻撃が成立します。

wIPS はクライアント認証プロセスを追跡し、アクセス ポイントに対する DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションが検出されると、攻撃検知および統計的シグニチャ照合プロセスが開始されます。DoS 攻撃が検出されると wIPS アラームが発行されます。このアラームには、標準のアラーム詳細記述とターゲット デバイス情報が含まれます。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、NCS オンライン ヘルプを参照してください。

この項では、アクセス ポイントに対する DoS 攻撃について説明します。この項は次のトピックで構成されています。

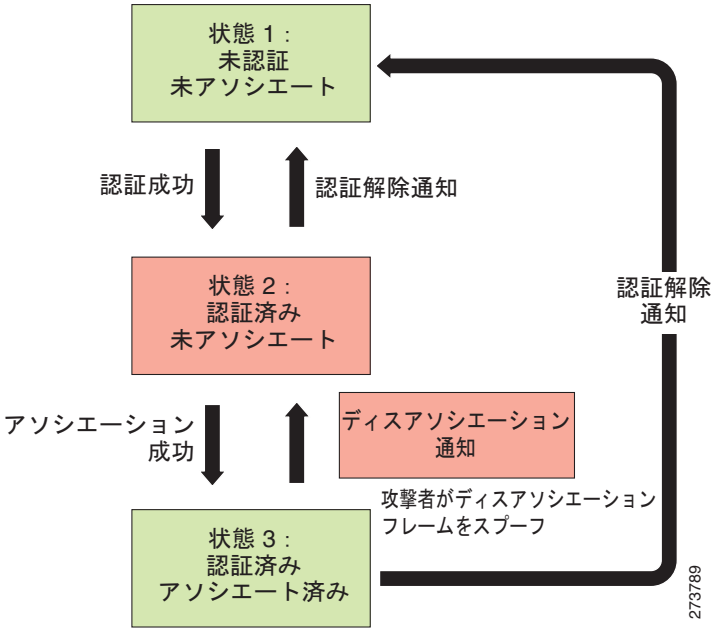
DoS 攻撃：アソシエーション フラッド

アラームの説明と考えられる原因

この DoS 攻撃は、アクセス ポイントに大量のスプーフィングされたクライアント アソシエーションを送り付け、アクセス ポイント リソース（特にクライアント アソシエーション テーブル）を枯渇させます。802.11 層では共有キー認証に欠陥があるため、この認証が使用されることはほとんどありません。別の方法として、802.1x や VPN などの高度な認証を利用するオープン認証（Null 認証）が使用されることがあります。オープン認証では、すべてのクライアントを認証してアソシエートできます。攻撃者はこの脆弱性を利用して大量のクライアントをエミュレートし、多数のクライアントを作成して、

ターゲット アクセス ポイントのクライアント アソシエーション テーブルのフラッディングを発生させます。クライアント アソシエーション テーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなり、DoS 攻撃が成立します（図 A-1 を参照）。

図 A-1　　アソシエーション フラッド



wIPS による解決

wIPS はこの DoS 攻撃を検出するために、クライアント アソシエーションが正常に完了した後で、スプーフィングされた MAC アドレスを検出し、802.1x アクションとデータ通信を追跡します。wIPS によりこの攻撃が報告されたら、このアクセス ポイントにログインし、アソシエーション テーブルでクライアント アソシエーションの数を検査します。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

DoS 攻撃：アソシエーション テーブル オーバーフロー

アラームの説明と考えられる原因

ワイヤレス侵入者は、スプーフした MAC アドレスを使って多数のワイヤレス クライアントを偽装し、アクセス ポイントのリソース（最も重要なのものとしてクライアント アソシエーション テーブル）を枯渇させます。それぞれの偽装クライアントがターゲット アクセス ポイントとのアソシエートと認証を試行します。通常、802.11 認証は完了します。これは、ほとんどのデプロイメントでは 802.11 オープン システム認証（Null 認証プロセス）が採用されているためです。このような偽装クライアントとのアソシエートの後に認証プロセスが実行されます。ただし偽装クライアントは 802.1x や VPN のような高度な認証は行わないため、プロトコル トランザクションが未完了状態になります。この時点で、攻撃を受けたアクセス ポイントでは各偽装クライアントのステートがクライアント アソシエーション

テーブルに維持されます。アクセス ポイントのリソースとクライアント アソシエーション テーブルがこのような偽装クライアントとそのステート情報でいっぱいになるため、攻撃を受けたアクセス ポイントは正規のクライアントに対処できなくなります。このようにして DoS 攻撃が成立します。

wIPS による解決

wIPS はクライアント認証プロセスを追跡し、アクセス ポイントに対する DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションにより、wIPS の攻撃検知および統計的シグニチャ照合プロセスが開始されます。

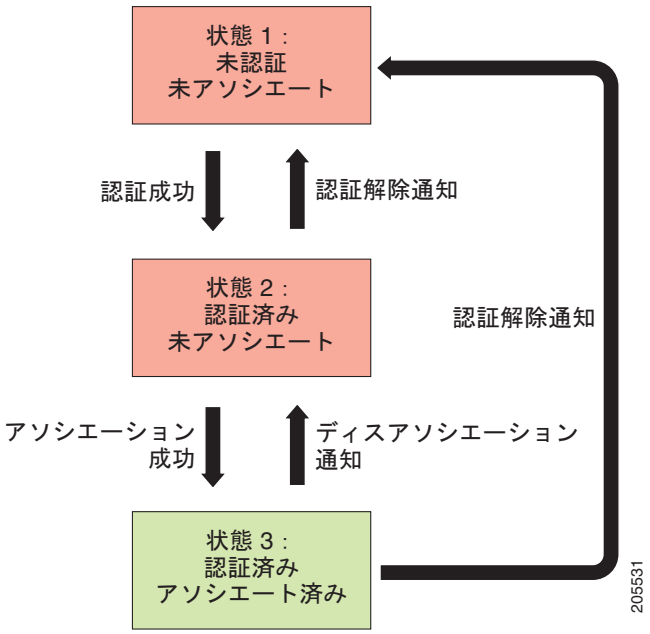
DoS 攻撃：認証フラッディング

攻撃ツール：Void11

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に準拠してこのようなステート マシンを実装しています（図 A-2 を参照）。アクセス ポイントでは各クライアントのステートがアクセス ポイントのクライアント テーブル（アソシエーション テーブル）に記録されます。この記録されるステートのサイズは制限されています。この制限は、ハードコーディングされた数値または物理メモリ制約に基づく数値のいずれかです。

図 A-2　認証フラッド



この DoS 攻撃は、多数のクライアント ステーションを偽装（MAC アドレス スプーフィング）してアクセス ポイントに認証要求を送信し、アクセス ポイントのクライアント ステート テーブル（アソシエーション テーブル）のフラッディングを引き起こします。ターゲット アクセス ポイントでは、個々の認証要求を受け取るたびにアソシエーション テーブルに状態 1 のクライアント項目が作成されます。オープン システム認証が使用されているアクセス ポイントは、*認証成功* フレームを戻し、クライアントを状態 2 にします。共有キー認証が使用されているアクセス ポイントは、攻撃者が偽装しているクライアントに*認証チャレンジ*を送信します。この場合攻撃者から応答はありません。この場合アクセ

ス ポイントはクライアントを状態 1 のままにします。いずれの場合でも、アクセス ポイントに状態 1 または状態 2 のクライアントが多数あり、アクセス ポイント アソシエーション テーブルがいっぱいになります。テーブルが上限に達すると、正規のクライアントがこのアクセス ポイントに対して認証およびアソシエートできなくなります。これにより DoS 攻撃が成立します。

wIPS による解決

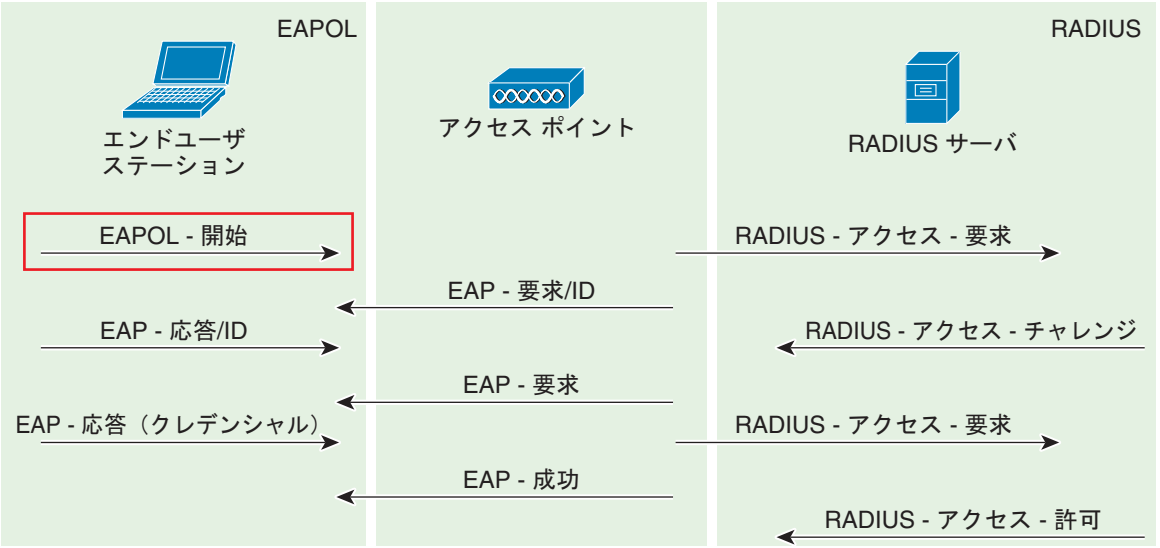
wIPS はこの DoS 攻撃を検出するため、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ アナリストはそのアクセス ポイントにログオンして現在のアソシエーション テーブルのステータスを確認できます。

DoS 攻撃：EAPOL-Start 攻撃

アラームの説明と考えられる原因

IEEE 802.1x 標準は、EAP over LAN（EAPOL）を使用して認証プロトコルを定義します。802.1x プロトコルは、クライアント ステーションから送信された EAPOL-Start フレームで認証トランザクションを開始します。アクセス ポイントは EAPOL-start フレームに対し EAP ID 要求および内部リソース割り当てによって応答します（図 A-3 を参照）。

図 A-3　EAPOL-Start プロトコルおよび EAPOL-Start 攻撃



攻撃者は、アクセス ポイントに EAPOL-start フレームを大量に送り付け、アクセス ポイント内部リソースを枯渇させることでアクセス ポイントを妨害しようとします。

wIPS による解決

wIPS はこの DoS 攻撃を検出するため、802.1x 認証状態遷移および特定の攻撃シグニチャを追跡します。

DoS 攻撃：PS ポール フラッド攻撃

アラームの説明と考えられる原因

電源管理は、おそらくワイヤレス LAN デバイスにおいて最も重要な機能の 1 つです。電源管理は、ステーションを長期にわたり省電力モードで維持し、アクセス ポイントから特定の間隔でのみデータを受信するようにすることで、電力を節約します。

ワイヤレス クライアント デバイスはアクセス ポイントに対し、スリープ モード（省電力モード）になる期間を通知する必要があります。この期間が終わるとクライアントは再起動し、待機データ フレームがあるかどうかを確認します。アクセス ポイントとのハンドシェイクが完了すると、データ フレームを受信します。アクセス ポイントからのビーコンには、クライアントが再起動してマルチキャスト トラフィックを受け入れる必要がある時点でクライアントにその旨を通知する Delivery Traffic Indication Map（DTIM）も含まれています。

アクセス ポイントは引き続き、スリープ中のワイヤレス クライアントのためにデータ フレームをバッファします。アクセス ポイントは Traffic Indication Map（TIM）を使用してワイヤレス クライアントに対しアクセス ポイントにデータがバッファされていることを通知します。マルチキャスト フレームは、DTIM を通知するビーコンの後に送信されます。

クライアントは、PS-Poll フレームを使用してアクセス ポイントへバッファ フレームを配信することを要求します。すべての PS-Poll フレームに対し、アクセス ポイントはデータ フレームで応答します。ワイヤレス クライアントのためにバッファされているフレームが多数ある場合、アクセス ポイントはフレーム応答のデータ ビットを設定します。その後、クライアントは次のデータ フレームを取得するために別の PS-Poll フレームを送信します。この処理は、バッファされたデータをすべて受信するまで行われます。

ハッカーがワイヤレス クライアントの MAC アドレスをスプーフし、大量の PS-Poll フレームを送信することがあります。この場合アクセス ポイントはバッファ データ フレームをワイヤレス クライアントに送信します。実際には、クライアントは省電力モードになっておりデータ フレームを受信しないことがあります。

wIPS による解決

wIPS は、ワイヤレス クライアントが正規のデータを失う可能性があるこの DoS 攻撃を検出できます。デバイスを特定し、ワイヤレス環境から削除します。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

DoS 攻撃：未認証アソシエーション

アラームの説明と考えられる原因

この DoS 攻撃では、アクセス ポイントに大量のスプーフィングされたクライアント アソシエーションを送り付け、アクセス ポイントのリソース（特にクライアント アソシエーション テーブル）を枯渇させます。802.11 層では共有キー認証に欠陥があるため、この認証が使用されることはほとんどありません。別の方法として、802.1x や VPN などの高度な認証を利用するオープン認証（Null 認証）が使用されることがあります。オープン認証では、すべてのクライアントを認証してアソシエートできます。攻撃者はこの脆弱性を利用して大量のクライアントを偽装し、多数のクライアントを作成して、ターゲット アクセス ポイントのクライアント アソシエーション テーブルのフラッディングを発生させます。クライアント アソシエーション テーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなり、DoS 攻撃の原因となります。

wIPS による解決

wIPS はこの DoS 攻撃を検出するために、クライアント アソシエーションが正常に完了した後で、スプーフィングされた MAC アドレスを検出し、802.1x アクションとデータ通信を追跡します。wIPS によりこの攻撃が報告されたら、このアクセス ポイントにログインし、アソシエーション テーブルでクライアント アソシエーションの数を検査します。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

DoS 攻撃：プローブ要求フラッド

アラームの説明と考えられる原因

この DoS 攻撃では、攻撃者は存在しないクライアントに供給するワイヤレス パケットの一定のストリームをターゲット AP に処理させます。プローブ要求フラッドの間、攻撃者は特定の AP を対象にした大量のプローブ要求を生成します。一般的なワイヤレスの設計では、AP がプローブ応答を送信することでプローブ要求に応答するように指定します。この応答には、企業ネットワークに関する情報が含まれます。フラッド攻撃中に大量のプローブ要求が送信されるため、AP は連続的に応答するためにスタックします。そのため、その AP に依存しているすべてのクライアントのサービスが拒否されます。

wIPS による解決

wIPS サーバは、検出されたプローブ要求フレームのレベルをモニタして、しきい値を超えた場合にプローブ要求フラッド アラームを生成します。要求が有効な場合でも、大量のフレームが原因でワイヤレス アクティビティに問題が生じることがあります。その結果、問題となっているフレームの発生源を特定して、企業環境から削除する必要があります。

DoS 攻撃：再アソシエーション要求フラッド

この DoS 攻撃では、AP に大量のエミュレートおよびスプーフィングされたクライアント再アソシエーションを送り付け、AP のリソース（特にクライアント アソシエーション テーブル）を枯渇させます。802.11 層では共有キー認証に欠陥があるため、今後はこの認証が使用されることはほとんどありません。唯一の代替策は、802.1x や VPN などの高度な認証を利用するオープン認証（Null 認証）です。オープン認証では、すべてのクライアントを認証してアソシエートできます。攻撃者はこの脆弱性を利用して大量のクライアントをエミュレートし、多数のクライアントを状態 3 にしてターゲット AP のクライアント アソシエーション テーブルのフラッディングを発生させます（以下を参照）。クライアント アソシエーション テーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなり、DoS 攻撃が成立します。

wIPS による解決

wIPS サーバは、ネットワークの再アソシエーション要求のレベルをモニタして、しきい値を超えた場合にこのアラームを生成します。

インフラストラクチャに対する DoS 攻撃

アクセス ポイントやクライアント ステーションに対する攻撃の他に、ワイヤレス侵入者は RF スペクトラムまたはバックエンド認証 RADIUS サーバをターゲットにして DoS（サービス拒否）攻撃を行うことがあります。遠隔から高出力アンテナを使って RF ノイズを発生させることで、RF スペクトラム

を容易に妨害できます。DDoS（分散型サービス拒否）攻撃で複数のワイヤレス攻撃者がバックエンド RADIUS サーバに対して認証要求を送り付けると、この RADIUS サーバが過負荷になります。この攻撃を行う上で、認証が成功する必要はありません。

インフラストラクチャに対する DoS 攻撃には、次のタイプがあります。

- 「DoS 攻撃：CTS フラッディング」（P.A-9）
- 「DoS 攻撃：クイーンズランド工科大学により検出された脆弱性」（P.A-10）
- 「DoS 攻撃：RF 電波妨害攻撃」（P.A-11）
- 「DoS 攻撃：RTS フラッディング」（P.A-11）
- 「DoS 攻撃：仮想キャリア攻撃」（P.A-12）
- DoS 攻撃：ビーコン フラッド
- DoS 攻撃：MDK3-Destruction 攻撃

DoS 攻撃：CTS フラッディング

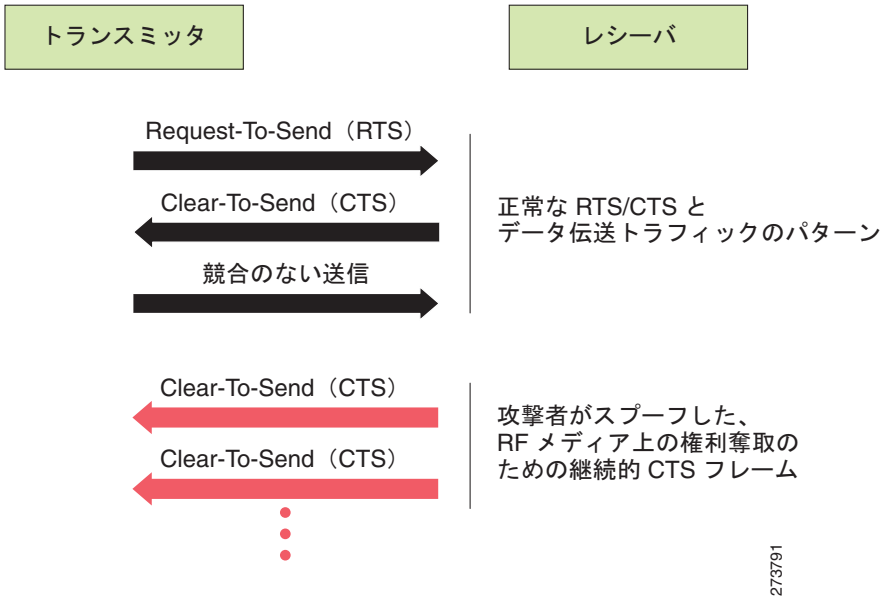
攻撃ツール：CTS Jack

アラームの説明と考えられる原因

IEEE 802.11 標準には、ステーションによる RF 媒体へのアクセスを制御する RTS/CTS（Request-To-Send/Clear-To-Send）機能がオプションとして含まれています。送信準備が整ったワイヤレス デバイスは、指定された期間にわたって RF 媒体への送信権限を獲得するため、RTS フレームを送信します。レシーバは同じ期間の CTS フレームを送信して RF 媒体への権限をトランスミッタに付与します。CTS フレームを監視するワイヤレス デバイスはすべて、競合がない状態で送信できるようにトランスミッタに対してこの媒体を生成します。

ワイヤレス DoS 攻撃を行うハッカーが、CTS フレームに付与された特権を悪用して RF 媒体を送信用に予約することがあります。攻撃者はバックツーバック CTS フレームを送信することで、攻撃者が CTS フレームの送信をやめるまで RF 媒体を共有する他のワイヤレス デバイスが送信を行わないようにできます（図 A-4 を参照）。

図 A-4　RF 制御に対する CTS スプーフとチャレンジ



wIPS による解決

wIPS は、DoS 攻撃に対する CTS フレームの乱用を検出します。

DoS 攻撃：クイーンズランド工科大学により検出された脆弱性

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02

アラームの説明と考えられる原因

802.11 WLAN デバイスは、基本アクセス メカニズムとしてキャリア検知多重アクセス / 衝突回避（CSMA/CA）を採用しています。このメカニズムでは、WLAN デバイスが送信開始前に媒体を待機し、すでに実行中の送信を検出するとバックオフします。衝突回避では、媒体が送信可能になる前の時点で物理検知メカニズムと Network Allocation Vector（NAV）を含む仮想検知メカニズムが組み合わせられます。DSSS プロトコルのクリア チャネル アセスメント（CCA）は、WLAN チャネルがクリアであり 802.11b デバイスがこのチャネルを介して送信できるかどうかを判断します。

802.11b プロトコル標準に DoS 無線周波数電波妨害攻撃を可能にする脆弱性があることが、オーストラリアのブリスベンにあるクイーンズランド工科大学 Information Security Research Centre 所属の Mark Looi、Christian Wullems、Kevin Tham、および Jason Smith により明らかになりました。

この攻撃では特に CCA 機能が攻撃を受けます。AusCERT の勧告では「この脆弱性に対する攻撃では、物理層の CCA 機能が悪用され、攻撃中に範囲内のすべての WLAN ノード（クライアントとアクセス ポイントの両方）によるデータ送信が遅延します。攻撃を受けたデバイスは、チャネルが使用中であるかのように動作し、ワイヤレス ネットワーク経由でのデータ送信が妨害されます。」と述べられています。

この DoS 攻撃は、IEEE 802.11、802.11b、および低速（20 Mbps 以下）802.11g ワイヤレス デバイスを含む DSSS WLAN デバイスに影響します。IEEE 802.11a（OFDM を使用）、高速（OFDM 使用で 20 Mbps を上回る速度）802.11g ワイヤレス デバイスはこの攻撃の影響を受けません。FHSS を使用するデバイスは影響を受けません。

攻撃者は WLAN カードを装着したラップトップや PDA を使い、SOHO WLAN と企業 WLAN に対してこの攻撃を行うことができます。この DoS 攻撃に対する唯一の回避策は、802.11a プロトコルに切り替えることです。

この DoS 攻撃の詳細については、次の URL を参照してください。

- www.isrc.qut.edu.au
- http://www.auscert.org.au/render.html?it=4091
- http://www.kb.cert.org/vuls/id/106678

wIPS による解決

wIPS は、この DoS 攻撃を検出して、アラームを発行します。当該デバイスを特定し、ワイヤレス環境から削除します。

DoS 攻撃：RF 電波妨害攻撃

アラームの説明と考えられる原因

WLAN の信頼性と効率は、無線周波数（RF）媒体の品質に基づきます。各 RF は RF ノイズの影響を受けます。攻撃者はこの WLAN の脆弱性を利用して 2 種類の DoS 攻撃を行う可能性があります。

- WLAN サービスの妨害：無免許の 2.4 GHz スペクトラムでは、攻撃が意図的ではないことがあります。コードレス電話、Bluetooth デバイス、電子レンジ、ワイヤレス監視ビデオ カメラ、ベビーモニタなどはすべて RF エネルギーを放出し、WLAN サービスを妨害する可能性があります。悪意のある攻撃では、高出力指向性アンテナを使用して 2.4 GHz または 5 GHz スペクトラムで RF 出力を操作し、遠隔から攻撃の影響を増幅させることができます。自由空間と建物内での減衰により、建物から 300 フィート離れた位置にある 1-kW 電波妨害デバイスは、オフィス エリアへ 50 ～ 100 フィートの電波妨害が可能です。同じ 1-kW 電波妨害デバイスを建物の中に配置すると、オフィス エリアへ 180 フィートの電波妨害が可能です。攻撃中は、ターゲット エリア内の WLAN デバイスはワイヤレス サービスを利用できません。
- 物理的な損傷を受けた AP ハードウェア：攻撃者は指向性高利得アンテナを備えた高出力トランスミッタをアクセス ポイントから 30 ヤード離れた位置で使い、アクセス ポイント内の電子部品に損害を与え、アクセス ポイントを永久に使用不能にするのに十分な RF 出力を発生できます。このような高エネルギー RF（HERF）ガンは効果的であり、安価で製作できます。

wIPS による解決

wIPS は、RF 電波妨害攻撃の可能性のある特定しきい値を超える連続 RF ノイズを検出します。

Cisco Spectrum Intelligence にも、802.11 非準拠電波妨害デバイスを検出する機能があります。Cisco Spectrum Intelligence の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

DoS 攻撃：RTS フラッディング

アラームの説明と考えられる原因

IEEE 802.11 標準には、ステーションによる RF 媒体へのアクセスを制御する RTS/CTS（Request-To-Send/Clear-To-Send）機能がオプションとして含まれています。送信準備が整ったワイヤレス デバイスは、指定された期間にわたって RF 媒体への送信権限を獲得するため、RTS フレームを

送信します。レシーバは同じ期間の CTS フレームを送信して RF 媒体への権限をトランスミッタに付与します。CTS フレームを監視するワイヤレス デバイスはすべて、競合がない状態で送信できるようにトランスミッタに対してこの RF 媒体を生成します。

ワイヤレス DoS 攻撃を行うハッカーが、CTS フレームに付与された特権を悪用して RF 媒体を送信用に予約することがあります。攻撃者は大きな送信期間テキスト ボックスを含むバックツーバック RTS フレームを送信して無線媒体を予約し、RF 媒体を共有する他のワイヤレス デバイスが送信を行わないようにします。

wIPS による解決

wIPS は、DoS 攻撃に対する RTS フレームの乱用を検出します。

DoS 攻撃：仮想キャリア攻撃

アラームの説明と考えられる原因

仮想キャリア検知攻撃を実行するには、ランダムな持続時間値を定期的に送信できるように 802.11 MAC 層実装を改ざんします。この攻撃は ACK、データ、RTS、および CTS フレームに対し、大きな持続時間値を使用して実行されます。これにより攻撃者は正規ユーザに対しチャネルへのアクセスを妨害できます。

通常の状況では、ACK フレームに大きな持続時間値が含まれているのは、ACK がフラグメンテーション パケット シーケンスの一部である場合だけです。データ フレームに大きな持続時間値が含まれているのは、そのデータ フレームがフラグメンテーション パケット交換の一部である場合だけです。

この攻撃への対処の 1 つとして、ノードにより受け入れられる持続時間値を制限する方法があります。この制限を超える大きな持続時間値が含まれているパケットはすべて、最大許容値になるように切り捨てられます。ロー キャップ値とハイ キャップ値が使用されます。ロー キャップの値は、ACK フレームの送信に必要な時間にフレームのメディア アクセス バックオフを加算した値です。ロー キャップが使用されるのは、監視対象パケットの後に送信可能なパケットが ACK または CTS のみである場合です。これには、RTS とすべての管理（アソシエーションなど）フレームが含まれます。ハイ キャップが使用されるのは、監視対象フレームの後にデータ パケットが送信可能である場合です。この場合の制限には、最大データ フレームの送信に必要な時間とそのフレームのメディア アクセス バックオフが含まれている必要があります。ハイ キャップを使用する必要があるのは、ACK 監視時（ACK が MAC レベルのフラグメンテーション パケットの一部である可能性があるため）と CTS 監視時です。

RTS フレーム受信するステーションはデータ フレームも受信します。IEEE 802.11 標準では、後続の CTS フレームとデータ フレームの正確な時間が指定されています。次のデータ フレームが受信されるかまたは受信されない時点まで、RTS の持続時間値が順守されます。監視対象 CTS が非請求であるか、または監視ノードが隠れ端末です。この CTS が有効な範囲内のステーション宛てである場合、有効なステーションは持続時間がゼロの Null ファンクション フレームを送信することでこれを無効にできます。この CTS が範囲外のステーション宛てである場合、防御策の 1 つとして、暗号を使用して署名された前の RTS のコピーを含む認証済み CTS フレームを導入する方法があります。この方法では、オーバーヘッドまたはフィジビリティの問題が発生する可能性があります。

wIPS による解決

wIPS は、この DoS 攻撃を検出します。デバイスを特定し、適切な手順でワイヤレス環境からそのデバイスを削除します。

DoS 攻撃：ビーコン フラッド

アラームの説明と考えられる原因

この DoS 攻撃では、攻撃者は存在しないクライアントに供給するワイヤレス パケットの一定のストリームをターゲット AP に処理させます。プローブ要求フラッドの間、攻撃者は特定の AP を対象にした大量のプローブ要求を生成します。一般的なワイヤレスの設計では、AP がプローブ応答を送信することでプローブ要求に応答するように指定します。この応答には、企業ネットワークに関する情報が含まれます。フラッド攻撃中に大量のプローブ要求が送信されるため、AP は連続的に応答するためにスタックします。そのため、その AP に依存しているすべてのクライアントのサービスが拒否されます。

wIPS による解決

wIPS サーバは、検出されたプローブ要求フレームのレベルをモニタして、しきい値を超えた場合にプローブ要求フラッド アラームを生成します。要求が有効な場合でも、大量のフレームが原因でワイヤレス アクティビティに問題が生じることがあります。その結果、問題となっているフレームの発生源を特定して、企業環境から削除する必要があります。

DoS 攻撃：MDK3-Destruction 攻撃

アラームの説明と考えられる原因

MDK3 はハッキング ツールのスイートであり、ユーザは企業のインフラストラクチャに対して多数の異なるセキュリティ突破方式を利用することができます。MDK3-Destruction モードは、ワイヤレス導入を効果的かつ完全にシャットダウンするために一連のツールを使用するスイートの特定の実装です。MDK-Destruction 攻撃の間、ツールは次のことを同時に行います。

- ビーコン フラッド攻撃を開始して、環境内に疑似 AP を作成する。
- 有効な企業 AP に対して認証フラッド攻撃を起動して、それらの AP がクライアントにサービスを提供しないようにする。
- 有効なクライアントとのすべてのアクティブな接続を切る。

追加の機能拡張により、ツールを使用して、ビーコン フラッドで生成された疑似 AP に有効なクライアントを接続できるため、環境内でさらなる混乱が生じます。

wIPS による解決

wIPS サーバは、MDK3-Destruction 攻撃の症状の組み合わせをモニタして、検出時にアラームを生成します。この攻撃はワイヤレス導入に多大な影響を及ぼす可能性があるため、通常のネットワーク オペレーションを再開するために、攻撃の発生源を特定し、ただちに削除することを強く推奨します。

クライアント ステーションに対する DoS 攻撃

ワイヤレス クライアント ステーションに対する DoS 攻撃は通常、802.11 管理フレームと 802.1x 認証プロトコルには暗号化メカニズムがないためにスプーフィング可能であるという事実に基づいて実施されます。たとえば、ワイヤレス侵入者はアクセス ポイントからクライアント ステーションへの 802.11 ディスアソシエーション フレームまたは認証解除フレームを継続的にスプーフィングすることで、クライアント ステーションへのサービスを妨害できます。

802.11 認証およびアソシエーション ステート攻撃の他に、802.1x 認証でも同様の攻撃シナリオがあります。たとえば 802.1x EAP-Failure メッセージまたは EAP-logoff メッセージは暗号化されていないため、これらのメッセージをスプーフして 802.1x 認証済みステートを妨害し、ワイヤレス サービスを妨害できます。

Cisco Adaptive Wireless IPS はクライアント認証プロセスを追跡し、DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションが検出されると、攻撃検知および統計的シグニチャ照合プロセスが開始されます。DoS 攻撃が検出されると wIPS アラームが発行されます。このアラームには、標準のアラーム詳細記述とターゲット デバイス情報が含まれます。

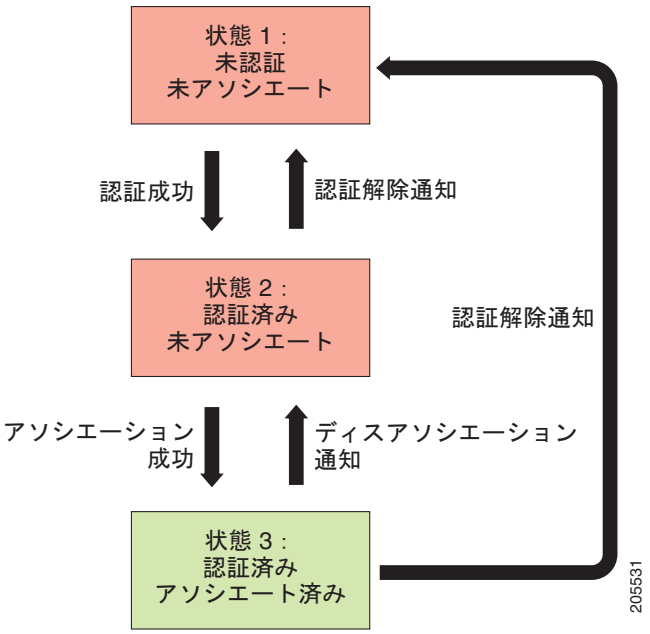
クライアント ステーションに対する DoS 攻撃には、次のタイプがあります。

DoS 攻撃：認証失敗攻撃

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは IEEE 標準に基づいてこのクライアント ステート マシンを実装します（図 A-5 を参照）。適切にアソシエートされたクライアントは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアントは、認証され状態 3 にアソシエートされるまでは WLAN データ通信プロセスに参加できません。IEEE 802.11 ではオープン システム認証と共有キー認証という 2 種類の認証サービスが定義されています。ワイヤレス クライアントはいずれかの認証プロセスによってアクセス ポイントにアソシエートされます。

図 A-5　認証失敗攻撃



この DoS 攻撃では、状態 3 のアソシエートされているクライアントからアクセス ポイントへ送信される無効な認証要求フレームが（不正な認証サービスおよびステータス コードで）スプーフィングされます。アクセス ポイントは無効な認証要求を受信するとクライアントを状態 1 に更新し、これによりクライアントのワイヤレス サービスが切断されます。

wIPS による解決

wIPS は、この DoS 攻撃を検出するためスプーフィングされた MAC アドレスと認証失敗をモニタします。このアラームは侵入が試みられたことを示すこともあります。アクセス ポイントとの認証段階でワイヤレス クライアントの失敗回数が多すぎると、サーバは侵入者がセキュリティを侵害しようとしている可能性を示すため、このアラームを生成します。

（注）　このアラームは、IEEE 802.11 の認証方式（オープン システムと共有キーなど）を対象にしています。EAP および 802.1x ベースの認証は、他のアラームによってモニタされます。

DoS 攻撃：ブロック ACK フラッド

アラームの説明と考えられる原因

この DoS 攻撃では、攻撃者は 802.11n AP を妨害し、特定の有効な企業クライアントからフレームを受信できないようにします。802.11n 規格の導入に伴い、クライアントがフレームの大きなブロックをセグメントに分割することなく、同時に送信することができるトランザクション メカニズムが導入されました。この交換を開始するために、クライアントは、送信ブロックのサイズを AP に知らせるシーケンス番号が含まれている Add Block Acknowledgement（ADDBA）を AP に送信します。AP は指定されているシーケンス内のすべてのフレームを受け入れ（範囲外のフレームはすべて削除し）、トランザクションが完了したら BlockACK メッセージをクライアントに送信します。

攻撃者はこのプロセスを悪用するために、有効なクライアントの MAC アドレスをスプーフィングしている間に無効な ADDBA フレームを送信できます。このプロセスにより、AP は無効なフレーム範囲の終わりに達するまで、クライアントから送信される有効なトラフィックを無視することになります。

wIPS による解決

wIPS サーバはスプーフされたクライアント情報の署名を確認するため ADDBA トランザクションをモニタします。攻撃者がブロック ACK 攻撃を開始しようとしていることが検出されると、アラームが生成されます。危険性のあるデバイスを特定し、特定したら早急にワイヤレス環境からそのデバイスを削除することを推奨します。

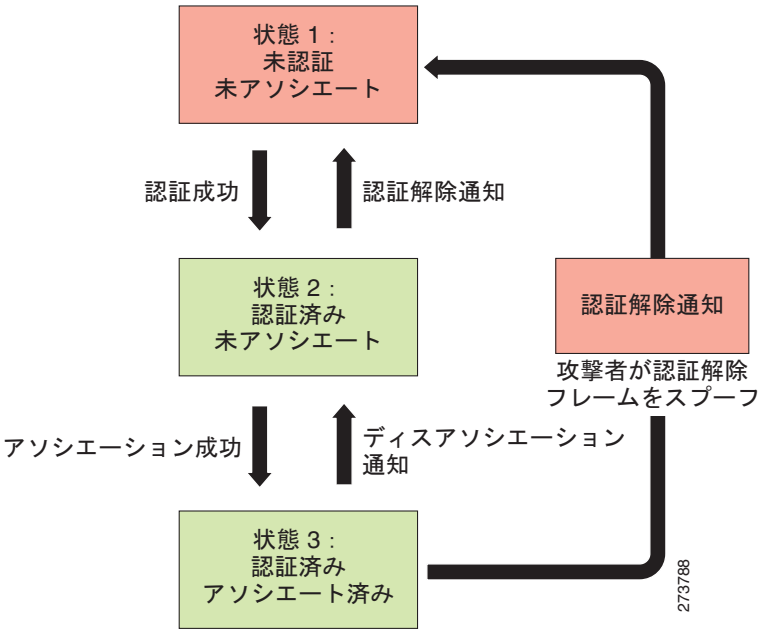
DoS 攻撃：De-Auth ブロードキャスト フラッド

攻撃ツール：WLAN Jack、Void11、Hunter Killer

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアントは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアントは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません（図 A-6 を参照）。

図 A-6　認証解除ブロードキャスト攻撃



この DoS 攻撃は、アクセス ポイントからブロードキャスト アドレスへの認証解除フレームをスプーフして、アクセス ポイントのすべてのクライアントを状態 1（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃は複数クライアントに対してワイヤレス サービスを妨害する点で非常に効果的であり即効性があります。通常、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフィングされた認証解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ アナリストは、そのアクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『Cisco Wireless Control System Configuration Guide』または WCS オンライン ヘルプを参照してください。

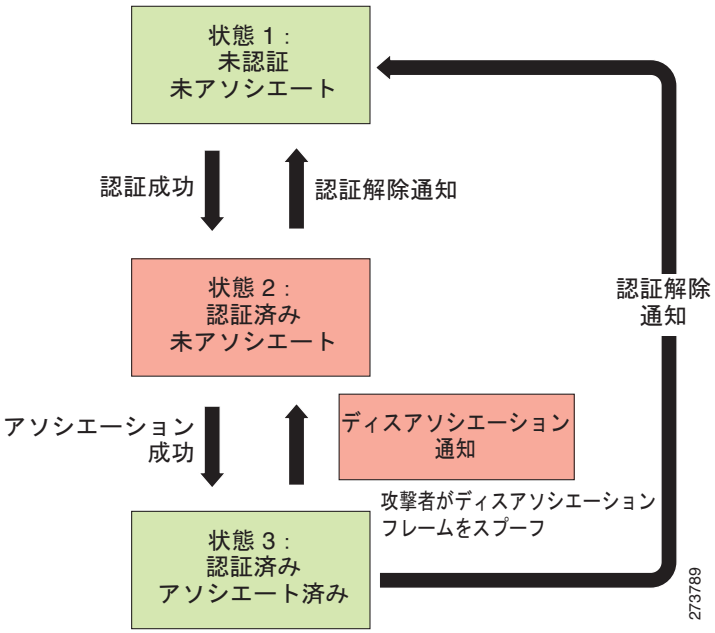
DoS 攻撃：De-Auth フラッド

攻撃ツール：WLAN Jack、Void11

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアントは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアントは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません（図 A-7 を参照）。

図 A-7　認証解除フラッド攻撃



この DoS 攻撃では、アクセス ポイントからクライアント ユニキャスト アドレスへの認証解除フレームをスプーフィングしてアクセス ポイントのクライアントを状態 1（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃はクライアントに対するワイヤレス サービスを妨害する点で非常に効果的かつ即効性があります。通常、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返し認証解除フレームをスプーフし、すべてのクライアントを使用不能な状態にします。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフィングされた認証解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントとクライアントが特定されます。WLAN セキュリティ オフィサは、アクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『Cisco Wireless Control System Configuration Guide』または WCS オンライン ヘルプを参照してください。

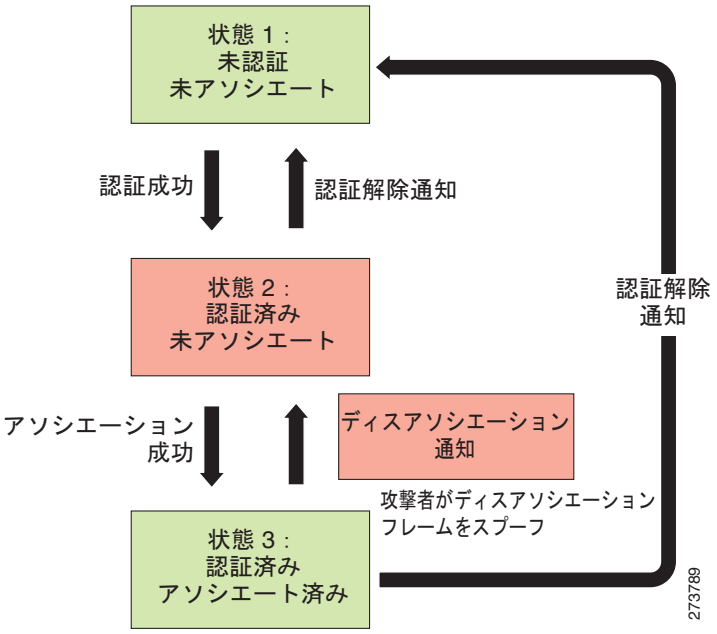
DoS 攻撃：ディスアソシエーション ブロードキャスト フラッド

攻撃ツール：ESSID Jack

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアント ステーションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません（図 A-8 を参照）。

図 A-8　ディスアソシエーション ブロードキャスト攻撃



この DoS 攻撃では、アクセス ポイントからブロードキャスト アドレス（すべてのクライアント）へのディスアソシエーション フレームをスプーフィングしてアクセス ポイントのクライアントを状態 2（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃は複数クライアントに対してワイヤレス サービスを妨害する点で効果的かつ即効性があります。通常、クライ

アント ステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、すべてのクライアントを使用不能な状態にします。

wIPS による解決

wIPS はこの DoS 攻撃を検出するため、スプーフィングされたディスアソシエーション フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ オフィサはアクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

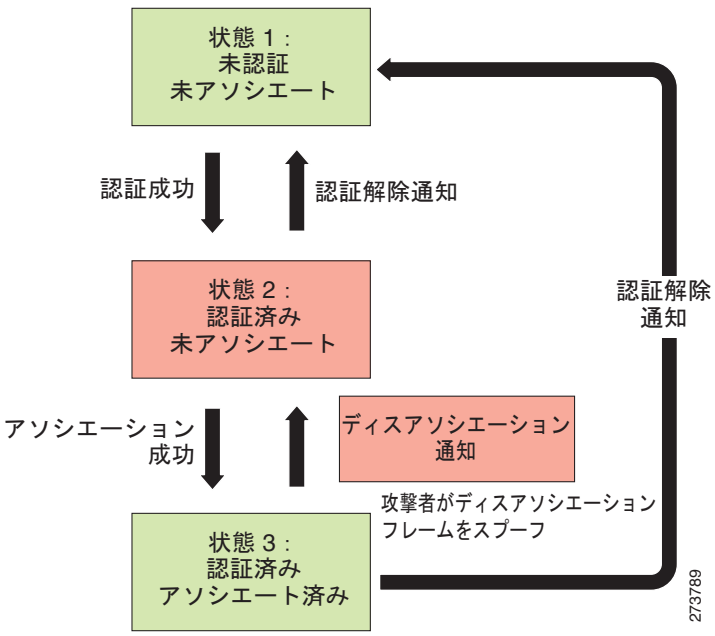
DoS 攻撃：Dis-Assoc フラッディング

攻撃ツール：ESSID Jack

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアントは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアントは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません（図 A-9 を参照）。

図 A-9　ディスアソシエーション フラッド攻撃



この DoS 攻撃では、アクセス ポイントからクライアントへのディスアソシエーション フレームをスプーフしてアクセス ポイントを状態 2（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃はこのクライアントに対してワイヤレス サービスを妨害する点で効果的

かつ即効性があります。通常、クライアント ステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、クライアントを使用不能な状態にします。

wIPS による解決

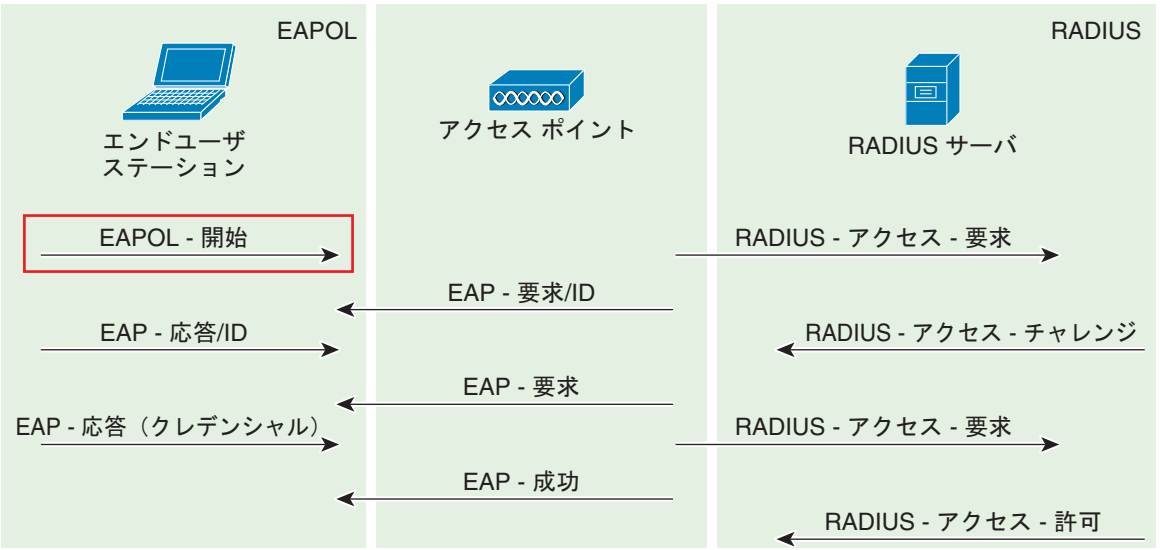
wIPS はこの DoS 攻撃を検出するため、スプーフィングされたディスアソシエーション フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ オフィサはアクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

DoS 攻撃：EAPOL-Logoff 攻撃

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol (EAP) over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、認証トランザクションを開始する EAPOL-start フレームで開始します。認証セッションの終了時にクライアント ステーションがログオフするときに、クライアント ステーションは 802.1x EAPOL-logoff フレームを送信し、アクセス ポイントとのセッションを終了します（図 A-10 を参照）。

図 A-10　EAPOL-Logoff 攻撃



EAPOL-logoff フレームは認証されないため、攻撃者はこのフレームをスプーフし、ユーザをアクセス ポイントからログオフさせることができます。これにより DoS 攻撃が成立します。クライアントがアクセス ポイントからログオフしたことは、クライアントが WLAN 経由で通信を試行するまでは明らかではありません。通常この妨害が検出されると、クライアントはワイヤレス接続を回復するため自動的に再アソシエートと認証を行います。攻撃者はスプーフィング EAPOL-logoff フレームを継続的に送信することで、この攻撃の効果を維持できます。

wIPS による解決

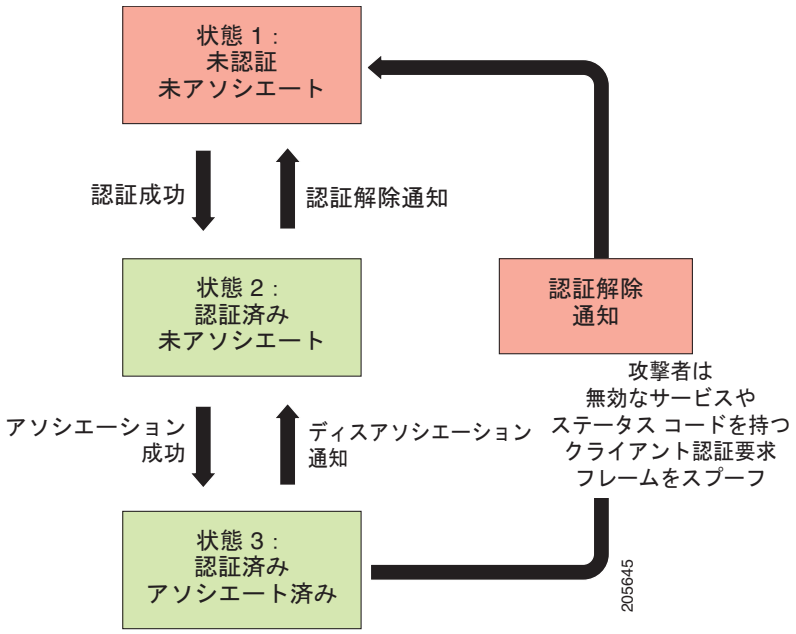
wIPS はこの DoS 攻撃を検出するため、802.1x 認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたクライアントとアクセス ポイントが特定されます。WLAN セキュリティ オフィサはこのアクセス ポイントにログオンして現在のアソシエーション テーブルのステータスを確認できます。

DoS 攻撃：FATA Jack ツールの検出

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは IEEE 標準に基づいてこのステート マシンを実装します。適切にアソシエートされたクライアント ステーションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信プロセスに参加できません。IEEE 802.11 ではオープン システムと共有キーという 2 種類の認証サービスが定義されています。ワイヤレス クライアントはいずれかの認証プロセスによってアクセス ポイントにアソシエートされます（図 A-11 を参照）。

図 A-11　無効な認証要求のスプーフィング



この DoS 攻撃では、状態 3 のアソシエートされているクライアントからアクセス ポイントへ送信される無効な認証要求フレームが（不正な認証サービスおよびステータス コードで）スプーフされます。アクセス ポイントは無効な認証要求を受信するとクライアントを状態 1 に更新しますが、これによりクライアント ワイヤレス サービスが切断されます。

FATA-jack は、同様の攻撃を実行するために最もよく使用されるツールの 1 つです。これは WLAN-jack を改変したツールであり、認証失敗パケットと、前回の認証失敗の理由コードをワイヤレス ステーションに送信します。これは、アクセス ポイントの MAC アドレスをスプーフィングした後に行われます。FATA-jack は最もアクティブな接続を閉じるため、時には、ユーザは通常の処理を続行するためにステーションをリブートする必要があります。

wIPS による解決

wIPS は、FATA-jack の利用を検出するためスプーフィングされた MAC アドレスと認証失敗をモニタします。このアラームは侵入が試みられたことを示すこともあります。アクセス ポイントとの認証段階でワイヤレス クライアントの失敗回数が多すぎると、wIPS は侵入者がセキュリティを侵害しようとしている可能性を示すため、このアラームを生成します。

（注）　このアラームは、802.11 の認証方式（オープン システムと共有キーなど）を対象にしています。EAP および 802.1x ベースの認証は、他のアラームによってモニタされます。

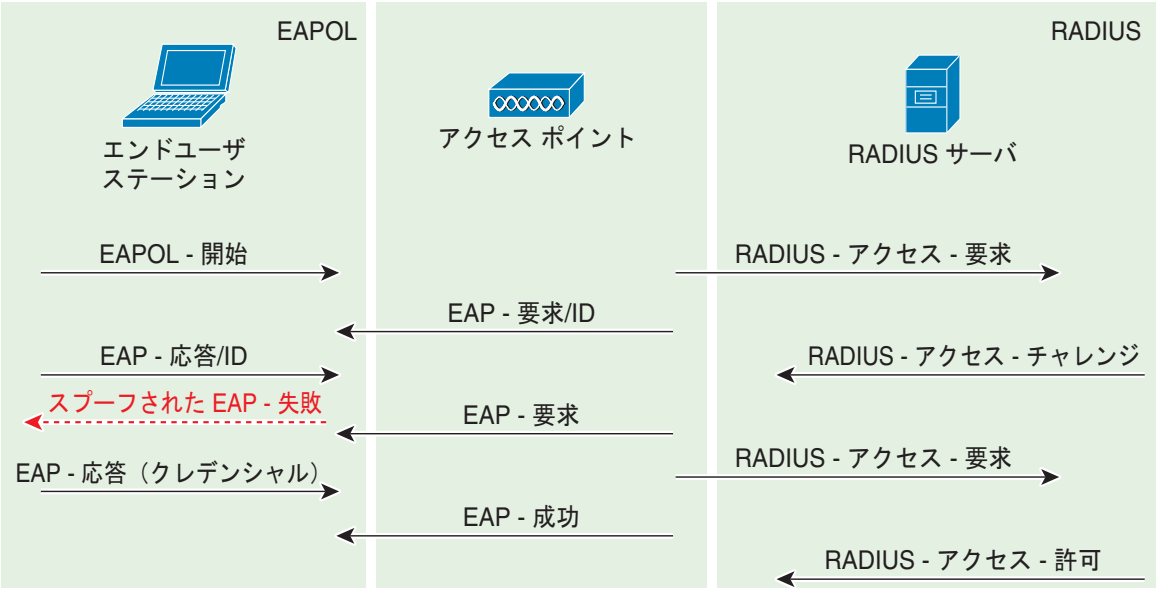
また、Cisco 管理フレーム保護は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

DoS 攻撃：不完全な EAP-Failure

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、認証トランザクションを開始する EAPOL-Start フレームで開始します。バックエンド RADIUS サーバとの 802.1x 認証パケット交換が完了すると、アクセス ポイントからクライアントに対し、認証の成功を示す EAP-success または失敗を示す EAP-failure が送信されます（図 A-12 を参照）。

図 A-12　不完全な EAP-Failure 攻撃



IEEE 802.1X 仕様では、必要な相互認証が完了していない場合にクライアントによるインターフェイスの表示が禁止されています。これにより、適切に実装された 802.1x クライアント ステーションが、不完全な EAP-success パケットを送信する疑似アクセス ポイントにだまされることを回避できます。

攻撃者はアクセス ポイントからクライアントへの不完全な EAP-failure フレームを継続的にスプーフィングしてクライアントの認証ステートを妨害し、クライアント インターフェイスが表示されないようにします。

wIPS による解決

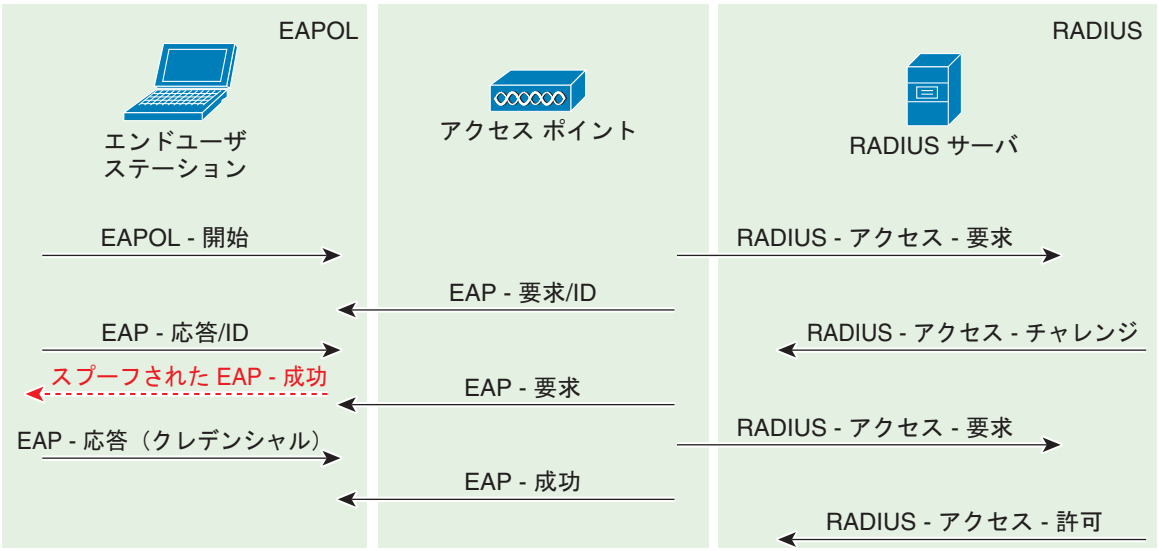
wIPS は、スプーフィングされた不完全な EAP-failure フレームと各クライアント ステーションおよびアクセス ポイントの 802.1x 認証ステートを追跡することで、この DoS 攻撃を検出します。デバイスを特定してワイヤレス環境から削除します。

DoS 攻撃：不完全な EAP-Success

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、認証トランザクションを開始する EAPOL-start フレームで開始します。バックエンド RADIUS サーバとの 802.1x 認証パケット交換が完了すると、アクセス ポイントからクライアントに対し、認証が正常に完了したことを示す EAP-success フレームが送信されます（図 A-13 を参照）。

図 A-13　EAP-Success 攻撃



IEEE 802.1X 仕様では、必要な相互認証が完了していない場合にクライアントによるインターフェイスの表示が禁止されています。これにより、適切に実装された 802.1x クライアント ステーションが、不完全な EAP-success パケットを送信して相互認証プロセスを迂回する疑似アクセス ポイントにだまされることを回避できます。

攻撃者はアクセス ポイントからクライアントへの不完全な EAP-success フレームを継続的にスプーフして認証ステートを妨害し、クライアント インターフェイスが表示されないようにします。

wIPS による解決

wIPS は、スプーフィングされた不完全な EAP-success フレームと各クライアント ステーションおよびアクセス ポイントの 802.1x 認証ステートを追跡することで、この DoS 攻撃を検出します。デバイスを特定してワイヤレス環境から削除します。

DoS 攻撃：プローブ応答フラッド

アラームの説明と考えられる原因

この DoS 攻撃では、攻撃者はステーションを有効な企業 AP にアソシエートできないようにします。一般的なワイヤレス トランザクションでは、ステーションは AP とアソシエーションする場合、AP のネットワークに関する情報を取得するためにプローブ要求を送信します。その後、ステーションは AP からのプローブ応答フレームを待ちます。攻撃者は、無効なプローブ応答を環境に大量に送り付けることで、このプロセスを悪用し、ステーションが有効な AP からの応答を受信できないようにできます。結果として、そのステーションはワイヤレス ネットワークに接続できなくなり、DoS 攻撃が開始されます。

wIPS による解決

wIPS サーバは、検出されたプローブ応答フレームのレベルをモニタして、しきい値を超えた場合にプローブ要求フラッド アラームを生成します。応答が有効な場合でも、大量のフレームが原因でワイヤレス アクティビティに問題が生じることがあります。その結果、問題となっているフレームの発生源を特定して、企業環境から削除する必要があります。

侵入検知：セキュリティ突破

ワイヤレス侵入の 1 つに、WLAN 認証メカニズムを突破し、有線ネットワークまたはワイヤレス デバイスへのアクセスを獲得するものがあります。認証方式への辞書攻撃は、アクセス ポイントに対する一般的な攻撃の 1 つです。侵入者は、アクセス ポイントとのアソシエーション プロセス中にワイヤレス クライアント ステーションを攻撃することもあります。たとえば何も知らないワイヤレス クライアントに対する疑似アクセス ポイント攻撃により、そのクライアントが疑似アクセス ポイントにアソシエートすることがあります。この攻撃によって、侵入者はワイヤレス ステーションへのネットワーク アクセスを取得して、ファイル システムをハッキングできる可能性があります。その後、侵入者はそのステーションを使用して企業の有線ネットワークにアクセスできます。

セキュリティに対するこのような脅威は、相互認証と強力な暗号化手法を使用することで防止できます。wIPS は弱いセキュリティ構成と侵入攻撃の試みを検出します。wIPS は最良のセキュリティ ポリシー実装を検証し、侵入の試みを検出することで強力なワイヤレス セキュリティ保護を実現します。このような脆弱性や攻撃の試みが検出されると、wIPS はこのような侵入の試みを管理者に通知するアラームを生成します。

セキュリティ突破攻撃には、次のタイプがあります。

- ASLEAP ツール検出
- 不良 EAP-TLS フレーム
- 「Airsnarf 攻撃」（P.A-26）
- 「ChopChop 攻撃」（P.A-28）
- 「WLAN のセキュリティ異常による Day-Zero 攻撃」（P.A-29）
- 「デバイスのセキュリティ異常による Day-Zero 攻撃」（P.A-30）
- 「AP のデバイス プローブ」（P.A-31）
- 「EAP メソッドへの辞書攻撃」（P.A-33）
- 「802.1x 認証に対する EAP 攻撃」（P.A-34）
- 「疑似 AP の検出」（P.A-35）
- 「疑似 DHCP サーバの検出（潜在的なワイヤレス フィッシング）」（P.A-35）

ASLEAP ツール検出

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは、WEP キー クラッキング攻撃に対して脆弱です（詳細については『Weaknesses in the Key Scheduling Algorithm of RC4-I』（Scott Fluhrer、Itsik Mantin、Adi Shamir 著）を参照）。

シスコは、既存の 802.1x フレームワークを利用して WEP キー攻撃を回避する LEAP（Lightweight Extensible Authentication Protocol）を導入しました。Cisco LEAP ソリューションには、セッションごとまたはユーザ キーに基づいて動的な相互認証と設定可能な WEP セッション キー タイムアウトが含まれています。LEAP ソリューションは安定したセキュリティ ソリューションとして見なされており、容易に設定できます。

LEAP を実行する無線 LAN ネットワークを侵害するためオフライン辞書攻撃で LEAP パスワードを解読するハッキング ツールがあります。このツールは LEAP を採用している WLAN ネットワークを検出すると、ユーザを認証解除します。これによりユーザは再接続しなければならないため、ユーザ名とパスワードのクレデンシャルを入力します。ハッカーはネットワークへ再アクセスする正規ユーザのパケットをキャプチャします。その後攻撃者はトラフィックをオフラインで解析し、辞書の値をテストしてパスワードを推測できます。

ASLEAP ツールの主な機能を以下に示します。

- libpcap を使用して RFMON モードでワイヤレス インターフェイスからリアルタイムに読み取る。
- 1 つのチャネルをモニタするか、またはチャネル ホッピングを実行して LEAP を実行しているターゲット ネットワークを探す。
- LEAP ネットワークのユーザをアクティブに認証解除し、ユーザに再認証を実行させる。これにより LEAP パスワードを迅速にキャプチャできます。
- LEAP を実行していないユーザではなく、まだ確認されていないユーザのみを認証解除する。
- 保存されている libpcap ファイルを読み取る。

- ダイナミック データベース テーブルと索引を使用して大きなファイルを迅速に検索できるようにする。これにより、フラット ファイルの検索とは対照的に、最悪検索時間が .0015 % 短くなります。
- LEAP 交換情報のみを libpcap ファイルに書き込む。
- これは、ディスク スペースが少ないデバイス（iPaq など）で LEAP クレデンシャルをキャプチャするときに使用できます。キャプチャされた LEAP クレデンシャルは、辞書攻撃を実行するためにそのデバイスよりもストレージ リソースが多いシステムの libpcap ファイルに保存されます。
- このツールのソースと Win32 バイナリ ディストリビューションは http://asleap.sourceforge.net から入手できます。

シスコは、辞書攻撃を阻止する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）プロトコルを開発しました。EAP-FAST は中間者攻撃、辞書攻撃、パケットおよび認証偽造攻撃を阻止します。EAP-FAST では、クライアントとサーバ間に PAC（Protected Access Credential）を使用して相互認証するトンネルが作成されます。トンネル確立プロセスが完了したら、クライアントはユーザ名とパスワードのクレデンシャルを使用して認証されます。

EAP-FAST の特長を以下に示します。

- 独自のプロトコルではない。
- IEEE 802.11i 標準に準拠している。
- TKIP と WPA に対応している。
- 証明書を使用しないため複雑な PKI インフラストラクチャを回避する。
- PC および Pocket PC の複数のオペレーティング システムに対応している。

wIPS による解決

Cisco Adaptive Wireless IPS は ASLEAP ツールの認証解除シグニチャを検出します。検出すると、サーバはワイヤレス管理者に警告します。攻撃を受けたステーションのユーザはパスワードをリセットする必要があります。最良の ASLEAP ツール対処策は、企業 WLAN 環境で LEAP を EAP-FAST に置き換える方法です。

Cisco WCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、弱い暗号化または認証を使用するように設定されているアクセス ポイントを事前予防的に報告します。自動セキュリティ脆弱性スキャンの詳細については、Cisco WCS オンライン ヘルプを参照してください。

Airsnarf 攻撃

アラームの説明と考えられる原因

ホットスポットとは、Wi-Fi ネットワーク アクセスが一般向けに開放されている場所を指します。ホットスポットは空港、ホテル、喫茶店をはじめ、ビジネスマンが集まることが多い場所にあります。ホットスポットは出張旅行者にとって最も重要なネットワーク アクセス サービスです。

ワイヤレス対応ラップトップや携帯機器から正規のアクセス ポイントに接続してサービスを利用できます。ほとんどのホットスポットでは、ユーザがアクセス ポイントに接続するときには、ログイン用の Web ページを開く操作以外の高度な認証メカニズムは不要です。ログインできるかどうかの条件は、利用者が利用料金を支払っているかどうかだけです。ワイヤレス ホットスポット環境では誰も信用すべきではありません。現在のセキュリティ上の懸念から、一部の WLAN ホットスポット ベンダーはユーザ ID の検証に 802.1x 以上の認証メカニズムを採用しています。

ホットスポット ネットワークの 4 つの基本コンポーネントは、次のとおりです。

- ホットスポット利用ユーザ：ワイヤレス対応のラップトップまたは携帯機器を所持し、ホットスポット ネットワークにアクセスするための有効なログイン情報を持つユーザ。
- WLAN アクセス ポイント：ホットスポット実装に応じて、スモール オフィス/ホーム オフィス（SOHO）ゲートウェイまたはエンタープライズ レベル アクセス ポイントのいずれかです。
- ホットスポット コントローラ：ユーザ認証、課金情報の収集、利用時間の追跡、機能のフィルタリングなどを実行します。これは独立したマシンであるか、またはアクセス ポイント自体に組み込まれています。
- 認証サーバ：利用ユーザのログイン クレデンシャルが保管されています。ほとんどのホットスポット コントローラは、認証サーバを使用して利用ユーザのクレデンシャルを検証します。

Airsnarf は、ハッカーがパブリック ワイヤレス ホットスポットからユーザ名とパスワードのクレデンシャルをどのように盗むことができるかを示すワイヤレス アクセス ポイント セットアップ ユーティリティです。

Airsnarf はシェル スクリプト ベースのツールであり、ユーザがログイン情報を入力するキャプティブ ポータルとホットスポットを作成します。ローカル ネットワーク情報、ゲートウェイ IP アドレス、SSID などの重要な値は airsnarf 設定ファイル内で設定できます。このツールは最初に、インターネットに接続されている認可済みのアクセス ポイントからホットスポット ワイヤレス クライアントをディスアソシエーションする非常に強力な信号をブロードキャストします。ワイヤレス クライアントは、何らかの不明な問題が原因でインターネットから一時的に切断されていると仮定して再度ログインしようとします。Airsnarf アクセス ポイントにアソシエートするワイヤレス クライアントが、ホットスポット オペレータにより導入された正規のアクセス ポイントではなく不正な Airsnarf アクセス ポイントから、IP アドレス、DNS アドレス、ゲートウェイ IP アドレスを受信します。Web ページからユーザ名とパスワードの入力が求められ、不正な Airsnarf アクセス ポイントによって DNS クエリが解決されます。ハッカーは入力されたユーザ名とパスワードを収集します。

そのユーザ名とパスワードは、ユーザに悪用を気づかれることなく、国内にある同じプロバイダーの他のホットスポット ロケーションで使用することができます。影響が小さくなる唯一のケースは、ホットスポット ユーザが利用時間課金制で接続している場合です。

Airsnarf ツールは、Airsnarf アクセス ポイントに知らないうちに接続しているラップトップ クライアントにも侵入する可能性があります。ハッカーは、http://airsnarf.shmoo.com/ から Airsnarf ツールをダウンロードすることができます。

wIPS による解決

wIPS は、Airsnarf ツールを実行しているワイヤレス デバイスを検出します。AirSnarf ツールを WLAN 環境から削除するために管理者が適切な措置をとる必要があります。

不良 EAP-TLS フレーム

アラームの説明と考えられる原因

有効な企業クライアントから AP への特定のフレーム送信により、データが不十分または無効なために、一部の AP モデルでクラッシュが生じることがあります。ワイヤレス攻撃者は、企業 AP をダウンさせるために、欠陥のあるフレームを送信することでこの脆弱性を悪用することができます。フラグを「c0」に設定した EAP-TLS パケットを送信し、TLS メッセージ長もデータも送信しないことで、一部のベンダーの AP は、リブートされるまで動作不能になることがあります。このリブート プロセスの間、攻撃者は企業ネットワークにアクセスする機会を得ることができ、セキュリティ リークとなる可能性があります。

wIPS による解決

wIPS サーバは、EAP-TLS の送信をモニタして、欠陥フレームや無効フレームを検出した場合にアラームを生成します。この問題は、必ずしもワイヤレス攻撃を示すものではありませんが、ワイヤレス導入全体の健全性を維持するためには修復する必要がある問題です。

ChopChop 攻撃

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは、さまざまな WEP クラッキング攻撃の対象となるリスクがあることはよく知られています。詳細については、『*Weaknesses in the Key Scheduling Algorithm of RC4 - I*』（Scott Fluhrer、Itsik Mantin、および Adi Shamir 著）を参照してください。

クラックされた WEP 秘密キーでは送信データは暗号化保護されず、データ プライバシーが侵害されます。WEP キーはユーザにより指定され、24 ビット IV（初期化ベクトル）にリンクされる秘密キーであり、ほとんどの場合 64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。chopchop ツールは Korek により Linux オペレーティング システム向けに開発されたツールで、WEP の脆弱性を悪用して WEP データ パケットの暗号化を解除します。ただし chopchop ツールはプレーンテキストのみを公開します。攻撃者は初期フェーズ中に以前にインジェクトされたパケットのパケット キャプチャ ファイルを使用し、改ざんしたパケットを攻撃対象ネットワークに再送信してパケットの暗号化を解除します。攻撃が完了すると、chopchop ツールは暗号化されていないパケット キャプチャ ファイルと、暗号化解除プロセスで判別された Pseudo Random Generation Algorithm（PRGA）情報を使用したもう 1 つのファイルを作成します。次に PGRA はプレーンテキストを取得するために暗号文と XOR されます。

次のコマンド例は、chopchop 攻撃を示しています。

```
aireplay-ng -4 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

値は次のとおりです。

4：chopchop 攻撃を示します

-h XX:XX:XX:XX:XX:XX：アソシエートされたクライアントの MAC アドレスを特定します

-b YY:YY:YY:YY:YY:YY：アクセス ポイントの MAC アドレスを特定します

ath0：ワイヤレス インターフェイス名を特定します

60 バイト未満のデータ パケットをドロップするアクセス ポイントは、この攻撃に対して脆弱ではありません。アクセス ポイントが 42 バイト未満のパケットをドロップする場合、aireplay はヘッダーが予測可能な限り、残りの欠落データを推測しようとします。IP パケットがキャプチャされると、ヘッダーの欠落部分を推測した後でヘッダーのチェックサムが正しいかどうかを検査します。攻撃者は 1 つ以上の WEP データ パケットを必要とします。chopchop 攻撃は動的 WEP 設定にも有効です。wIPS は、chopchop ツールを使用して潜在的な攻撃を検出できます。

wIPS による解決

wIPS は、潜在的な chopchop 攻撃が進行中の場合にアラートをアクティブにします。企業環境では WEP を使用しないでください。ネットワーク内でセキュリティ ホールが発生しないように適切な手段を講じ、よりセキュアな IEEE 802.11i 標準を使用するようにワイヤレス ネットワーク インフラストラクチャとデバイスをアップグレードしてください。

WLAN のセキュリティ異常による Day-Zero 攻撃

アラームの説明と考えられる原因

WLAN のパフォーマンス効率は、常に RF 環境の変動とクライアント デバイスの移動の影響を受けます。注意深くモニタされ、適切に調整されている WLAN システムでは、適切に管理されていない WLAN システムよりも高いスループットを実現できます。Cisco Unified Wireless Network に内蔵されている Radio Resource Management（RRM; 無線リソース管理）機能は、RF 環境をモニタし、この環境で検出されるパフォーマンスの問題を動的に修正します。さらなるパフォーマンス異常のモニタリングは、Wireless IPS システムを使用して行うことができます。RRM の詳細については、NCS オンライン ヘルプを参照してください。

wIPS は、WLAN を継続的にモニタし、ワイヤレス管理者に対して問題を警告する早期兆候を通知することで、WLAN のパフォーマンスと効率を維持します。パフォーマンスが低下すると生成されるパフォーマンス アラームは、次のカテゴリに分類されます。

- RF 管理：wIPS は物理 RF 環境をモニタします。この RF 環境は動的であり、WLAN パフォーマンスの問題の発生源となることがよくあります。RF 環境のモニタリング中に、サーバは以下の WLAN の基本情報を明らかにし、問題を報告します。
  - チャネルの干渉とチャネルの割り当ての問題
  - チャネル ノイズと非 802.11 信号
  - WLAN RF サービス対象エリア
  - 典型的な RF 隠れノードの問題
- 問題のあるトラフィック パターン：RF マルチパスの問題をはじめとする多くの WLAN パフォーマンスの問題は、MAC 層プロトコル トランザクションと統計に表れます。wIPS はワイヤレス トラフィックを追跡、分析することで、パフォーマンスの非効率性と低下を早期に検出できます。多くの場合、wIPS は検出されたパフォーマンスの問題の原因を判別し、対策を提案できます。wIPS は、次の項目を含む、MAC 層プロトコルの特性を追跡します。
  - フレーム CRC エラー
  - フレーム再送信
  - フレーム速度（1、2、5.5、11、... Mbps）の使用と分布
  - レイヤ 2 フレーム フラグメンテーション
  - アクセス ポイントとステーション アソシエーション、リレーションシップの再アソシエーションとディスアソシエーション
  - ローミング ハンドオフ
- チャネルまたはデバイスのオーバーロード：wIPS は、負荷をモニタおよび追跡して、チャネル帯域幅の制限と WLAN デバイスのリソース容量の両方でスムーズな運用ができるようにします。プロビジョニングの不足や過剰な増加のために、WLAN のパフォーマンスが十分でない場合、wIPS はアラームを生成して、詳細な情報を提供します。RF には、同僚が隣接チャネルに新しい WLAN デバイスを取り付けた場合でも、WLAN チャネルの使用率を大幅に増加させる境界はありません。wIPS は WLAN をモニタして、適切な帯域幅とリソースのプロビジョニングを確保します。
- 導入および動作エラー：wIPS はエアウェーブをスキャンして、設定エラーと動作エラーを検出します。次に示す領域は継続的にモニタされます。
  - 同一 SSID を使用するアクセス ポイント間の矛盾する設定
  - ベスト プラクティスの原則に違反する設定
  - クライアントおよびアクセス ポイントの設定の不一致が原因で発生する接続の問題
  - WLAN インフラストラクチャのデバイスのダウンまたはリセット

- WLAN デバイス実装の欠陥

- IEEE 802.11e および VoWLAN の問題：IEEE 802.11e 標準では、既存の 802.11 a/b/g ワイヤレス標準に加えて Quality of Service（QoS）機能とマルチメディア サポートが導入されました。これらの標準との完全な下位互換性を維持しながら、付加機能が追加されました。QoS 機能は、音声ビデオ アプリケーションで重要です。ワイヤレス LAN では帯域幅が制限されており、従来の有線イーサネットと比較するとオーバーヘッドが高くなっています。RTS/CTS メカニズム、パケット フラグメンテーション、パケット再送信、確認、コリジョンなど、さまざまな理由でスループットが低下します。

wIPS による解決

wIPS は、ワイヤレス ネットワーク上の多数のデバイスにおける 1 つのパフォーマンス侵害ポリシー違反を検出します。指定の期間内に特定のポリシーに違反しているデバイス数が検出されたか、またはアラームの閾値設定に指定されているデバイス数のパーセンテージが突然増加しています。パフォーマンス侵害違反によっては、詳しい分析のためにデバイスをモニタおよび特定することを推奨します。

例：

- 多数のデバイスによって「ステーションにより過負荷状態になったアクセス ポイント」アラームが生成される場合、ハッカーが数千のステーションを生成し、これらのステーションを企業アクセス ポイントに強制的にアソシエートしている可能性があります。この状況が発生すると、正規の企業クライアントがアクセス ポイントに接続できなくなります。
- ワイヤレス デバイスでフレーム再試行が過剰に行われる場合、ノイズ、干渉、パケット コリジョン、マルチパス、隠れノードの問題などが発生している可能性があります。

デバイスのセキュリティ異常による Day-Zero 攻撃

アラームの説明と考えられる原因

企業環境に WLAN を追加すると、ネットワーク セキュリティに対するまったく新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無認可のユーザに公開する可能性があります。個人の使用のために従業員によって設置された不正アクセス ポイントは通常、企業のセキュリティ ポリシーに準拠していません。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正なアクセス ポイントの他にも、ワイヤレス ネットワークのセキュリティを侵害するワイヤレス セキュリティの脆弱性（アクセス ポイントの設定ミス、未設定のアクセス ポイントなど）があります。さまざまなソースから企業ネットワークに対して DoS（サービス拒否）攻撃が行われることもあります。

NCS は、ワイヤレス インフラストラクチャ内でセキュリティの脆弱性を自動的に評価する機能を提供します。この機能は、セキュリティの脆弱性または設定ミスを事前に報告します。さらに詳細な評価が Wireless IPS システムから無線で行われることがあります。wIPS は、包括的なセキュリティ モニタリング テクノロジー スイートを使用して、次のカテゴリ内の 100 件を超えるさまざまな脅威状況をユーザに警告します。

- ユーザ認証とトラフィック暗号化（静的 WEP 暗号化、VPN、Fortress、Cranite、802.11i、802.1x）：このカテゴリ（認証と暗号化）の一般的なセキュリティ違反には、設定ミス、古いソフトウェア/ファームウェア、最適ではない企業セキュリティ ポリシーの選択などがあります。
- 不正デバイス、モニタ対象デバイス、アドホック モード デバイス：企業ネットワーク（ワイヤレスおよび有線）の整合性を保護するために、不正デバイスを検出し、即時に削除する必要があります。
- 設定の脆弱性：セキュアな WLAN においては強力な導入ポリシーを実装することが重要です。ただしポリシーを適用するには、設定ミスや装置ベンダーの実装エラーにより引き起こされる違反を定期的なモニタによって捕捉する必要があります。ラップトップに Wi-Fi 機能が内蔵される傾向が

高まっていることから、WLAN 設定の複雑さは、アクセス ポイントからユーザ ラップトップに拡大しています。WLAN デバイス設定管理製品を利用すると設定プロセスが容易になりますが、内蔵 Wi-Fi 機能が未使用、未設定の状態のラップトップでは特に検証を行う必要があります。

- セキュリティ突破に関する侵入検知：このワイヤレス侵入には、WLAN 認証メカニズムの突破による有線ネットワークまたはワイヤレス デバイスへのアクセスの獲得が含まれます。認証方式への辞書攻撃は、アクセス ポイントに対する非常に一般的な攻撃の 1 つです。侵入者は、アクセス ポイントとのアソシエーション プロセス中にワイヤレス クライアント ステーションを攻撃することもあります。たとえば何も知らないワイヤレス クライアントに対する疑似 AP 攻撃により、そのクライアントが疑似アクセス ポイントにアソシエートすることがあります。この攻撃によって、侵入者はワイヤレス ステーションへのネットワーク アクセスを取得して、ファイル システムをハッキングできる可能性があります。その後、侵入者はそのステーションを使用して企業の有線ネットワークにアクセスできます。
- DoS 攻撃の侵入検知：ワイヤレス DoS（サービス拒否）攻撃は、レイヤ 1 またはレイヤ 2 における WLAN のさまざまな脆弱性を悪用してワイヤレス サービスを妨害することを狙いとしています。DoS 攻撃は、物理的な RF 環境、アクセス ポイント、クライアント ステーション、またはバックエンド認証 RADIUS サーバをターゲットとする可能性があります。たとえば、オフィスがある建物の外部から、高出力指向性アンテナを使用した遠隔 RF 電波妨害攻撃が行われることがあります。侵入者が使用する攻撃ツールは、スプーフされた 802.11 管理フレームやスプーフされた 802.1x 認証フレームなどのハッキング技法、または単に総当たりのパケット フラッディング方法を利用します。

wIPS による解決

wIPS は、ワイヤレス ネットワーク上の多数のデバイスにおける 1 つのセキュリティ IDS/IPS ポリシー違反を検出します。指定の期間内に特定のポリシーに違反しているデバイス数が検出されたか、またはアラームの閾値設定に指定されているデバイス数のパーセンテージが突然増加しています。セキュリティ IDS/IPS 違反によっては、詳しい分析のためにデバイスをモニタおよび特定し、デバイスが企業ワイヤレス ネットワークを何らかの形（攻撃または脆弱性）で侵害していないかどうかを確認することを推奨します。不正デバイスの数が増加している場合は、ネットワークに対して攻撃が行われている可能性があります。WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、デバイスを検出する不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースします。

暗号化が無効な状態でクライアント デバイスの数が突然増加した場合は、企業セキュリティ ポリシーを再確認し、ポリシー ルールに基づいてユーザが最高レベルの暗号化と認証を強制的に使用するようにする必要があります。

AP のデバイス プローブ

よく使用されるスキャン ツールには、NetStumbler（新しいバージョン）、MiniStumbler（新しいバージョン）、MACStumbler、WaveStumbler、PrismStumbler、dStumbler、iStumbler、Aerosol、Boingo Scans、WiNc、AP Hopper、NetChaser、Microsoft Windows XP scan などがあります。

アラームの説明と考えられる原因

wIPS は WLAN をプローブし、アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を試行するワイヤレス デバイスを検出します。

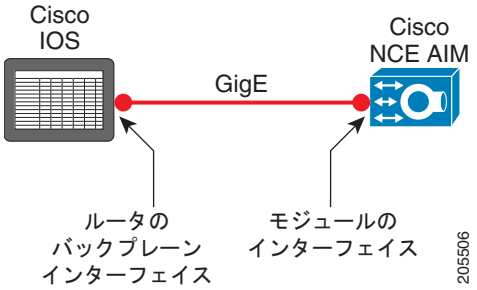
このようなデバイスは、次のいずれかの方法でセキュリティの脅威となる可能性があります。

- ウォードライビング、WiLDing（ワイヤレス LAN 検出）、ウォーチョーキング、ウォーサイクルイング、ウォーライトトレイリング、ウォーブッシング、ウォーフライング。
- 危険な無差別アソシエーションを試行する正規ワイヤレス クライアント。

ウォードライビング、ウォーチョーキング、ウォーウォーキング、ウォーフライングでは次のような行動が行われます。

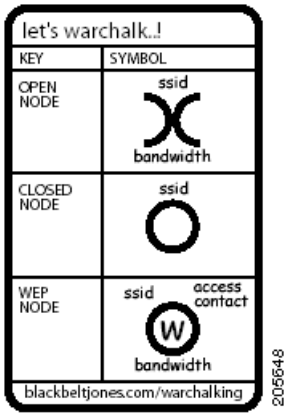
- ウォードライビング：ワイヤレス ハッカーがウォードライビング ツールを使用してアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティなどの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します（図 A-14 を参照）。

図 A-14　インターネットに投稿されたアクセス ポイント ロケーション



- ウォーチョーキング：ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に共通シンボルを使用して WLAN 設定をマーキングします（図 A-15 を参照）。

図 A-15　ウォーチョーキングで使用される共通シンボル



- ウォーウォーキング：ウォーウォーキングはウォードライビングに似ていますが、ハッカーが車ではなく徒歩で徘徊します。
- ウォーフライング：ウォーフライングは、ワイヤレス ネットワークを上空から探します。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています。

危険なアソシエートを試行する正規ワイヤレス クライアント

このアラームでのもう 1 つのセキュリティの脅威は、より深刻な損害をもたらす可能性があります。これらのアラームの一部は、使用可能なアクセス ポイント（ネイバーのアクセス ポイントやより深刻な損害をもたらす不正なアクセス ポイントを含む）にアソシエートしようとしている WLAN 上の正規の認可ワイヤレス クライアントによって発生することがあります。このセキュリティの脅威は、Wi-Fi カード内蔵 Windows XP ラップトップや、Boingo または WiNc クライアント ユーティリティなどのワイヤレス接続ツールを使用するラップトップに起因することがあります。このクライアント ステーションへのアソシエートが完了すると侵入者がこのクライアント ステーションにアクセスできるようになり、これが原因で重大なセキュリティ侵害が発生する可能性があります。さらにクライアント ステーションが意図しないアクセス ポイントと企業の有線 LAN を接続するブリッジとなることがあります。一般にラップトップには Wi-Fi カードが内蔵されており、またこのようなラップトップは企業内 WLAN ネットワークに物理的に接続しています。Windows ラップトップで Windows ブリッジ サービスが有効になっている場合は有線ネットワークが外部に公開されます。セキュリティ保護のため、すべてのクライアント ステーションに固有の SSID を設定し、意図しないアクセス ポイントからのアソシエートを防止します。また、802.1x やさまざまな EAP 方式などの相互認証を検討してください。

wIPS は、NetStumbler ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。ハッカーが最新バージョンの NetStumbler ツールを使っている場合、「アクセス ポイントをプローブするデバイス」アラームが生成されます。古いバージョンの場合、「NetStumbler の検出」アラームが生成されます。

NetStumbler は、ウォードライビングとウォーチョーキングに最も広く使用されているツールです。NetStumbler の Web サイトでは、ウォーウォーカーが重たいラップトップを持ち歩かずにすむように、Pocket PC ハードウェアで使用できる MiniStumbler ソフトウェアを提供しています。Windows 2000、Windows XP およびこれ以降のオペレーティング システムが稼働するマシンで実行できます。また、よく使用される別のスキャン ツールである Wellenreiter よりも多くのカードがサポートされます。ウォーウォーカーは、MiniStumbler や類似製品を使ってショッピングセンターや小売店舗を徘徊します。

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。wIPS を使用して、ビーコンでそれぞれの SSID をブロードキャスト（アナウンス）しているアクセス ポイントを確認します。

EAP メソッドへの辞書攻撃

アラームの説明と考えられる原因

EEE 802.1x は、ワイヤレス LAN および有線 LAN の認証の EAP フレームワークを規定しています。EAP フレームワークにより、柔軟な認証プロトコルを実装できます。一部の 802.1x または WPA 実装では LEAP、MD5、OTP（ワンタイム パスワード）、TLS、TTLS などの認証プロトコルが使用されています。このような認証プロトコルの一部で使用されるユーザ名とパスワードのメカニズムでは、ユーザ名が暗号化されずに送信され、認証チャレンジへの応答にパスワードが使用されます。

ほとんどのパスワード ベースの認証アルゴリズムは、辞書攻撃の影響を受けます。辞書攻撃では攻撃者が暗号化されていない 802.1x ID プロトコル交換からユーザ名を獲得します。その後攻撃者は一般的なパスワードの辞書のすべての単語またはパスワードの可能な組み合わせからユーザのパスワードを推測してネットワーク アクセスを獲得しようとします。辞書攻撃は、パスワードに一般的な単語、名前、またはこの両方の組み合わせとわずかな変更（末尾の 1 桁または 2 桁の番号など）が使用されることに依存しています。

辞書攻撃がオンラインでアクティブに行われる場合、攻撃者はあらゆるパスワードの組み合わせを繰り返し試行します。オンライン辞書攻撃を防止するには、認証サーバ（RADIUS サーバ）で使用可能なロックアウト メカニズムを利用し、無効なログインの試みが特定の回数を超えた後にユーザをロックアウトします。辞書攻撃はオフラインで行われることもあります。この場合、攻撃者は正常に完了した認証チャレンジ プロトコル交換をキャプチャし、チャレンジ応答に対してあらゆるパスワードの組み合わせを突き合わせます。オンライン攻撃とは異なり、オフライン アタックは容易に検出されません。強力なパスワード ポリシーを採用し、定期的にユーザ パスワードの有効期限が切れるように設定することで、オフライン攻撃ツールによる攻撃の成功率を大幅に削減します。

wIPS による解決

wIPS はオンライン辞書攻撃を検出するため、802.1x 認証プロトコル交換とユーザ ID の利用状況を追跡します。辞書攻撃が検出されると、ユーザ名と攻撃ステーションの MAC アドレスがアラーム メッセージに示されます。

wIPS は、ユーザ名とパスワードに基づく認証方式から、シスコをはじめとする多くのベンダーによりサポートされている暗号化トンネルに基づく認証方式（PEAP や EAP-FAST など）に切り替えるように指示します。

802.1x 認証に対する EAP 攻撃

アラームの説明と考えられる原因

IEEE 802.1x は、ワイヤレス LAN および有線 LAN の認証の拡張認証プロトコル（EAP）フレームワークを定義します。EAP フレームワークにより、柔軟な認証プロトコルを実装できます。一部の 802.1x または WPA 実装では LEAP、MD5、OTP（ワンタイム パスワード）、TLS、TTLS、EAP-FAST などの認証プロトコルが使用されています。このような認証プロトコルの一部で使用されるユーザ名とパスワードのメカニズムでは、ユーザ名が暗号化されずに送信され、認証チャレンジへの応答にパスワードが使用されます。

ほとんどのパスワード ベースの認証アルゴリズムは、辞書攻撃の影響を受けます。辞書攻撃では攻撃者が暗号化されていない 802.1x ID プロトコル交換からユーザ名を獲得します。その後攻撃者は一般的なパスワードの辞書のすべての「単語」またはパスワードの可能な組み合わせからユーザのパスワードを推測してネットワーク アクセスを獲得しようとします。辞書攻撃は、パスワードに一般的な単語、名前、またはこの両方の組み合わせと一部の変更（末尾の 1 桁または 2 桁の番号など）がよく使用されることに依存しています。

正規の 802.1x ユーザ ID とパスワードの組み合わせ（または有効な証明書）を使用する侵入者は、正確な EAP タイプを理解していなくても 802.1x 認証プロセスを突破できます。侵入者はさまざまな EAP（TLS、TTLS、LEAP、EAP-FAST、PEAP など）を使ってネットワークへのログオンを試みます。攻撃者がネットワークへの認証を試す EAP の種類が限られていることから、これは試行錯誤による攻撃です。

wIPS による解決

wIPS は、攻撃者がさまざまな 802.1x 認証タイプを使用してネットワークにアクセスしようとする試みを検出します。適切な手順に従ってデバイスを特定し、ワイヤレス環境から削除してください。

疑似 AP の検出

アラームの説明と考えられる原因

疑似 AP ツールは、NetStumbler、Wellenreiter、MiniStumbler、Kismet などを使うウォードライバを混乱させるおとりとして動作して WLAN を保護します。このツールは数千もの偽の 802.11b アクセス ポイントを模倣してビーコン フレームを生成します。ウォードライバは大量のアクセス ポイントを検出すると、ユーザが実際に導入している実際のアクセス ポイントを特定できません。このツールはウォードライバを阻止するには非常に有効ですが、帯域幅消費、正規クライアント ステーションの誤誘導、WLAN 管理ツールとの干渉といったデメリットがあります。WLAN 内で疑似 AP ツールを実行することは推奨しません。

wIPS による解決

管理者は疑似 AP ツールを実行するデバイスを特定してワイヤレス環境から削除する必要があります。

疑似 DHCP サーバの検出（潜在的なワイヤレス フィッシング）

アラームの説明と考えられる原因

ネットワーク上のデバイスへの動的 IP アドレスの割り当てにはダイナミック ホスト コンフィギュレーション プロトコル（DHCP）が使用されます。

DHCP アドレス割り当ては次のように行われます。

ステップ 1　クライアント NIC から、DHCP サーバの IP アドレスが必要であることを示す DHCP 検出パケットが送信されます。

ステップ 2　サーバは IP アドレスを含む DHCP オファー パケットを送信します。

ステップ 3　クライアント NIC が DHCP 要求を送信します。この要求は DHCP サーバに対し、サーバ オファーにより送信された IP アドレスをクライアントに割り当てることを求めます。

ステップ 4　サーバは、NIC から特定の IP アドレスに対する要求が送信されたことを確認する DHCP ACK を戻します。

ステップ 5　クライアントのインターフェイスが、DHCP サーバから最初に提供された IP アドレスを割り当てるかまたはバインドします。

DHCP サーバは専用マシンとし、企業内有線ネットワークの一部にする必要があります。また、ワイヤレス ゲートウェイおよび有線ゲートウェイにすることもできます。その他のワイヤレス デバイスでは、DHCP サービスが無害な状態で実行される場合と、WLAN IP サービスを妨害する目的で悪意を持って実行される場合があります。ワイヤレス クライアントにはサーバを認証する機能がないため、DHCP サーバの IP アドレスを要求するワイヤレス クライアントは、このような疑似 DHCP サーバに接続してこの疑似サーバの IP アドレスを取得する可能性があります。このような疑似 DHCP サーバはクライアントに対して機能しないネットワーク設定が提供するか、またはすべてのクライアント トラフィックを疑似サーバ経由にすることがあります。これで、ハッカーはクライアントから送信されるすべてのパケットを盗聴できます。ハッカーは不正な DNS サーバを利用して偽の Web ページ ログインにユーザを誘導し、ユーザ名とパスワードのクレデンシャルを取得しようとします。DoS 攻撃のために、機能しないルーティング不可能な IP アドレスを提供することもあります。通常、このような攻撃は暗号化されていない WLAN（ホットスポットやトレードショー ネットワークなど）が対象となります。

wIPS による解決

wIPS は、DHCP サービスを実行し、気づいていないユーザに IP アドレスを提供するワイヤレス STA を検出します。

クライアントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、デバイスを検出します。

高速 WEP クラック（ARP リプレイ）ツールの検出

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは WEP キー クラッキング攻撃に対して脆弱であることがよく知られています（『*Weaknesses in the Key Scheduling Algorithm of RC4 - I*』（Scott Fluhrer、Itsik Mantin、および Adi Shamir 著）を参照）。

攻撃者によって WEP 秘密キーがクラックされると、暗号化による保護がなくなり、結果としてデータ プライバシーが侵害されます。WEP キーはユーザにより指定され、24 ビット IV（初期化ベクトル）にリンクされる秘密キーで構成され、ほとんどの場合 64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。送信ステーションが決定する IV を頻繁に再利用したり、連続するフレームで再利用したりできるので、ワイヤレス侵入者がこの秘密キーを復元できる可能性が高まります。

WEP キーに対する攻撃で最も重要な点は、キーのサイズです。十分な固有 IV の数は、64 ビット WEP キーで約 15 万、128 ビット WEP キーで約 50 万から 100 万です。トラフィックが不十分な場合に、ハッカーはこのような攻撃を行うために十分なトラフィックを生成する手法を編み出しています。これは、arp-request パケットに基づくリプレイ アタックと呼ばれます。このようなパケットの長さは一定であるため、容易に検出できます。1 つの正規 arp-request パケットをキャプチャして繰り返し再送信すると、他のホストは暗号化された応答で対応し、新しい（そして弱い場合もある）IV を提供します。

wIPS による解決

wIPS は弱い WEP 実装について警告し、IV 使用の問題を訂正するためのデバイス ファームウェア アップグレードがデバイス ベンダーからリリースされている場合はこのアップグレードを推奨します。企業 WLAN ネットワークで TKIP（Temporal Key Integrity Protocol）暗号化メカニズムを使用して WEP の脆弱性を保護することが理想的です。TKIP はほとんどのエンタープライズ レベル ワイヤレス装置でサポートされています。TKIP 対応デバイスはこのような WEP キー攻撃の対象となりません。

NCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、弱い暗号化または認証を使用する設定されているアクセス ポイントを事前予防的に報告します。自動セキュリティ脆弱性スキャンの詳細については、NCS オンライン ヘルプを参照してください。

フラグメンテーション攻撃

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは、さまざまな WEP クラッキング攻撃の対象となるリスクがあることはよく知られています。詳細については、『*Weaknesses in the Key Scheduling Algorithm of RC4 - I*』（Scott Fluhrer、Itsik Mantin、および Adi Shamir 著）を参照してください。

クラックされた WEP 秘密キーでは送信データは暗号化保護されず、データ プライバシーが侵害されます。WEP キーはユーザにより指定され、24 ビット IV（初期化ベクトル）にリンクされる秘密キーであり、ほとんどの場合 64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。

http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation によれば、aircrack プログラムはパケットからわずかな量のキー関連情報を収集し、ARP パケットまたは LLC パケット（あるいはこの両方）を判明している情報と共にアクセス ポイントに送信します。パケットがアクセス ポイントから正常にエコーバックされると、戻されるパケットからより多くのキー関連情報を取得できます。PRGA の 1500 バイト（場合によっては 1500 バイト未満）分を取得するまで、このサイクルが繰り返されます。

この攻撃では WEP キー自体は復元されず、PRGA が取得されるだけです。packetforge-ng によってさまざまなインジェクション攻撃に使用できるパケットが生成されるときにこの PRGA を使用できます。

次のコマンド例は、フラグメンテーション攻撃を示しています。

```
aireplay-ng -5 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

値は次のとおりです。

5：フラグメンテーション攻撃を示します

-h XX:XX:XX:XX:XX:XX：アソシエートされたクライアントの MAC アドレスを特定します

-b *YY:YY:YY:YY:YY:YY*：アクセス ポイントの MAC アドレスを特定します

ath0：ワイヤレス インターフェイス名を特定します

wIPS による解決

wIPS は、Wi-Fi ネットワークに対して進行中の潜在的なフラグメンテーション攻撃を検出します。さらに、wIPS は、企業環境では WEP を使用しないよう勧告を行います。適切な手段を講じて、ネットワーク内でのセキュリティ ホールの発生を防ぎ、よりセキュアな IEEE 802.11i 標準を使用できるようにワイヤレス ネットワーク インフラストラクチャとデバイスをアップグレードすることを促します。

HT-Intolerant Degradation of Service

アラームの説明と考えられる原因

802.11n の実装には、レガシー実装よりもワイヤレス範囲と速度を大幅に向上できる可能性がありますが、これらの利点は、1 台でもレガシー デバイスがネットワークに導入されると、簡単に失われたり、相殺されたりします。この状況を回避するために、wIPS サーバは、n 個の対応デバイス間において n 以下の速度で送信されているパケットを検出した場合に、HT-Intolerant Degradation of Service アラームを生成します。

wIPS による解決

このサービスの低下は必ずしもワイヤレス攻撃を示すものではありませんが、伝送速度の低下はネットワークのパフォーマンスに悪影響を及ぼすことがあります。そのため、ユーザは 802.11n の最適な導入を維持するために、レガシー デバイスを特定して取り除く必要があります。

ハニーポット AP の検出

アラームの説明と考えられる原因

企業環境に WLAN を追加すると、ネットワーク セキュリティに対するまったく新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無認可のユーザに公開する可能性があります。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険

にさらされる可能性があります。不正アクセス ポイントの脅威以外にも、アクセス ポイントの設定ミスや未設定、DoS（サービス拒否）攻撃といったさまざまなワイヤレス セキュリティ リスクや侵入の可能性が存在します。

企業のワイヤレス ネットワークを対象とする最も効果的な攻撃の 1 つに、「ハニー ポット」アクセス ポイントを使用した攻撃があります。攻撃者は NetStumbler、Wellenreiter、MiniStumbler などのツールを使い、企業アクセス ポイントの SSID を検出します。次に建物の外（可能な場合は同じ建物の中）にアクセス ポイントをセットアップし、検出した企業 SSID をブロードキャストします。何も知らないクライアントが、信号強度が高いこの「ハニー ポット」アクセス ポイントに接続します。アソシエートが完了すると、トラフィックが「ハニー ポット」アクセス ポイントを経由するため、攻撃者はクライアント ステーションに対して攻撃を実行します。

wIPS による解決

Cisco Adaptive Wireless IPS により「ハニー ポット」アクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

Hot-Spotter ツールの検出（潜在的なワイヤレス フィッシング）

アラームの説明と考えられる原因

ホットスポットとは、Wi-Fi ネットワーク アクセスが一般向けに開放されている場所を指します。ホットスポットは空港、ホテル、喫茶店をはじめ、ビジネスマンが集まることが多い場所にあります。現在、ホットスポットは出張旅行者にとっては最も重要なネットワーク アクセス サービスです。正規のアクセス ポイントに接続してサービスを利用するには、ワイヤレス対応ラップトップまたは携帯機器が必要です。ほとんどのホットスポットでは、ユーザがアクセス ポイントに接続するときには、ログイン用の Web ページを開く操作以外の高度な認証メカニズムは不要です。ログインできるかどうかの条件は、利用者が利用料金を支払っているかどうかだけです。ワイヤレス ホットスポット環境では誰も信用すべきではありません。現在のセキュリティ上の懸念から、一部の WLAN ホットスポット ベンダーはユーザ ID の検証に 802.1x 以上の認証メカニズムを採用しています。

WLAN ホットスポット ネットワークの基本コンポーネント

ホットスポット ネットワークの 4 つの基本コンポーネントは、次のとおりです。

- ホットスポット利用ユーザ：ワイヤレス対応のラップトップまたは携帯機器を所持し、ホットスポット ネットワークにアクセスするための有効なログイン情報を持つユーザ。
- WLAN アクセス ポイント：ホットスポット実装に応じて、SOHO ゲートウェイまたはエンタープライズ レベル アクセス ポイントのいずれかです。
- ホットスポット コントローラ：ユーザ認証、課金情報の収集、利用時間の追跡、機能のフィルタリングを実行します。これは独立したマシンであるか、またはアクセス ポイント自体に組み込まれています。
- 認証サーバ：利用ユーザのログイン クレデンシャルが保管されています。ほとんどの場合、ホットスポット コントローラは認証サーバを使用して利用ユーザのクレデンシャルを検証します。

Hotspotter は、採用されている暗号メカニズムに依存せずに、ワイヤレス クライアントに対する侵入操作を自動化します。攻撃者は Hotspotter ツールを使用してワイヤレス ネットワークでプローブ要求フレームを受動的にモニタし、Windows XP クライアント ネットワークの SSID を特定します。

攻撃者は優先ネットワーク情報を獲得した後に、提供されるよく使用されるホットスポット ネットワーク名のリストに対してネットワーク名（SSID）を照合します。一致するネットワーク名が見つかると、Hotspotter クライアントがアクセス ポイントとして動作します。クライアントはこの状況を知らずにこの疑似アクセス ポイントを認証してアソシエートします。

クライアントがアソシエートされたら、DHCP デーモンやその他のスキャンを新たなターゲットに対して実行するコマンド（スクリプトなど）を実行するように Hotspotter ツールを設定できます。

異なる環境（ホームとオフィスなど）で稼働しているが、Windows XP ワイヤレス接続設定で同じホットスポット SSID を使用するように設定されているクライアントも、この攻撃の影響を受けます。クライアントはその SSID を使用してプローブ要求を送信するため、ツールに対して脆弱になります。

wIPS による解決

wIPS により不正なアクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

Identical Send and Receive Address

アラームの説明と考えられる原因

攻撃者は、企業ネットワーク内のワイヤレス アクティビティを抑制するために、ワイヤレス パケットを変更して（パケットの送信元および宛先 MAC 情報に対する変更など）、さまざまな異なる特性をエミュレートすることがよくあります。これらのフィールドが同一の場合、IT 担当者に潜在的な攻撃について警告するために Identical Send and Receive Address アラームが生成されます。

wIPS による解決

通常のネットワーク環境では、パケットの送信元と宛先が同一になることはありません。そのため、企業の管理者は迅速な措置をとり、変更されたパケットの根本原因を特定する必要があります。

Improper Broadcast Frames

アラームの説明と考えられる原因

802.11 の標準の導入では、特定のフレーム（ユニキャスト フレームとも呼ばれる、ACK など）を個別の宛先に送信し、他のフレームをワイヤレス導入内のすべての受信者に「ブロードキャスト」することができます。一般的に、この 2 つのカテゴリはオーバーラップできません。たとえば、Association Request フレームをすべてのリスニング デバイス向けのブロードキャストとして送信することはできません。このシナリオでは、wIPS サーバは、潜在的な問題をスタッフに警告するために Improper Broadcast Frames アラームを生成します。

wIPS による解決

Improper Broadcast Frames アラームは、チェックしないでおくとネットワークのパフォーマンスを妨げる可能性がある潜在的な攻撃を示します。無効なフレームの発信元を特定する手順を実行し、早急にそのフレームをワイヤレス環境から削除する必要があります。

Karma ツールの検出

アラームの説明と考えられる原因

Karma ツールを使用すると、ワイヤレス攻撃者は、検出されたプローブ要求に応答するソフト AP としてクライアントを設定できます。この実装は、複数の異なるネットワーク（仕事の場合は SSID「Corporate」、家庭での使用の場合は SSID「Home」など）に接続するように設定されているステーションからのクエリに応答するように設計されています。この例では、ソフト AP は、クライアントが

仕事中の場合に「Home」のプローブに応答するように設定することができます。この方法で、攻撃者は企業クライアントをだまし、潜在的に機密のネットワーク トラフィックを疑似 AP にルーティングします。

wIPS による解決

wIPS サーバは、企業環境内でこのツールを使用しているワイヤレス ステーションが検出されたときに Karma ツール アラームを生成します。ユーザは攻撃しているデバイスを特定して、ただちに取り除く必要があります。

不正 802.11 パケットの検出

アラームの説明と考えられる原因

不正なパケット（不正な非標準 802.11 フレーム）を使用するハッカーは、ワイヤレス デバイスを予期しない方法で動作させることができます。一部のベンダーのワイヤレス NIC のファームウェアは、不正なパケットによってクラッシュすることがあります。

このような脆弱性の例として、NULL プローブ応答フレーム（プローブ応答フレームの SSID が Null）や管理フレームの過大サイズの情報要素などがあります。このような不正なフレームがブロードキャストされると、複数のワイヤレス クライアントがクラッシュすることがあります。

wIPS による解決

wIPS は、一部の NIC のロックアップとクラッシュを引き起こす可能性がある不正なパケットを検出できます。また、攻撃を受けている間にブルー ページやロックアップの問題が発生するワイヤレス クライアントでは、WLAN NIC ドライバまたはファームウェアのアップグレードを検討する必要があります。

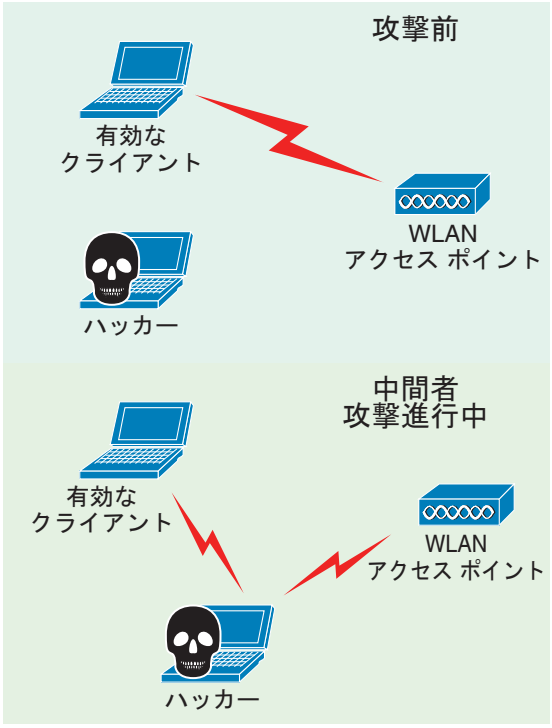
wIPS によりクライアントが特定、報告されると、WLAN 管理者はデバイス ロケータを使用してそのクライアントを見つけることができます。

中間者攻撃の検出

アラームの説明と考えられる原因

中間者（MITM）攻撃は、最も一般的な 802.11 攻撃の 1 つであり、企業の機密情報や個人情報がハッカーに漏れる可能性があります。MITM 攻撃ではハッカーは 802.11 ワイヤレス アナライザを使用し、WLAN 上で送信される 802.11 フレームをモニタします。ハッカーはアソシエーション フェーズでワイヤレス フレームをキャプチャし、ワイヤレス クライアント カードとアクセス ポイントの IP アドレスと MAC アドレスの情報、クライアント アソシエーション ID、ワイヤレス ネットワークの SSID を取得します（図 A-16 を参照）。

図 A-16　中間者攻撃



一般的な MITM 攻撃では、ハッカーがスプーフされたディスアソシエーション フレームまたは認証解除フレームを送信します。ハッカー ステーションがクライアントの MAC アドレスをスプーフし、アクセス ポイントとのアソシエートを継続します。同時にハッカーはスプーフされたアクセス ポイントを別のチャネルにセットアップし、クライアントとのアソシエーションを維持します。有効なクライアントとアクセス ポイント間のトラフィックはすべてのこのハッカーのステーションを経由します。

最もよく使用される MITM 攻撃ツールの 1 つに Monkey-Jack があります。

wIPS による解決

wIPS は、ハッカーによる MITM 攻撃を阻止するために強力な暗号化および認証メカニズムを使用することを推奨します。このような攻撃を回避する方法の 1 つに、MAC アドレス除外リストを使用し RF チャネル環境をモニタして、MAC アドレスのスプーフを防止する方法があります。

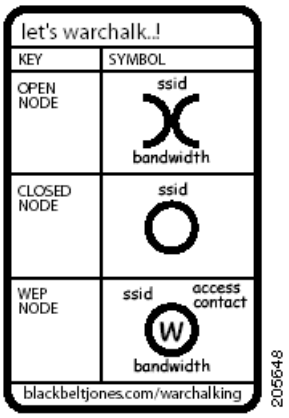
また、Cisco 管理フレーム保護（MFP）は MITM 攻撃に対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

NetStumbler の検出

アラームの説明と考えられる原因

wIPS は、NetStumbler ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。ハッカーが新しいバージョンの NetStumbler ツールを使っている場合、「*アクセス ポイントをプローブするデバイス*」アラームが生成されます。古いバージョンの場合、wIPS は *NetStumbler の検出*アラームを生成します（図 A-17 を参照）。

図 A-17　ウォーチョーキングで使用される共通シンボル



NetStumbler は、ウォードライビングとウォーチョーキングに最も広く使用されているツールです。ワイヤレス ハッカーがウォードライビング ツールを使用してアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、ハッカーが車ではなく徒歩で徘徊します。NetStumbler の Web サイトでは、ウォーウォーカーが重たいラップトップを持ち歩かずにすむように、Pocket PC ハードウェアで使用できる MiniStumbler ソフトウェアを提供しています。このツールは Windows 2000、Windows XP、およびこれ以降のバージョンが稼働するマシンで実行できます。また、よく使用される別のスキャン ツールである Wellenreiter よりも多くのカードがサポートされます。ウォーウォーカーは、MiniStumbler や類似製品を使ってショッピングセンターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。wIPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

NCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、SSID をブロードキャストするように設定されているアクセス ポイントをすべて報告します。自動セキュリティ脆弱性スキャンの詳細については、NCS オンライン ヘルプを参照してください。

NetStumbler 犠牲者の検出

アラームの説明と考えられる原因

wIPS は、NetStumbler ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。ハッカーが新しいバージョンの NetStumbler ツールを使っている場合、「アクセス ポイントをプローブするデバイス」アラームが生成されます。古いバージョンの場合、wIPS は NetStumbler の検出アラームを生成します。

NetStumbler は、ウォードライビング、ウォーウォーキング、ウォーチョーキングに最も広く使用されているツールです。ワイヤレス ハッカーがウォードライビング ツールを使用してアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセス ポイ

ントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、不正処理をハッカーが車ではなく徒歩で行います。NetStumbler の Web サイトでは、ウォーウォーカーが重たいラップトップを持ち歩かずにすむように、Pocket PC ハードウェアで使用できる MiniStumbler ソフトウェアを提供しています。このツールは Windows 2000、Windows XP、およびこれ以降のバージョンが稼働するマシンで実行できます。また、よく使用される別のスキャン ツールである Wellenreiter よりも多くのカードがサポートされます。ウォーウォーカーは、MiniStumbler や類似製品を使ってショッピングセンターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています。

wIPS による解決

wIPS は、NetStumbler を実行するステーションが企業アクセス ポイントにアソシエートされていることを検出すると、ユーザに対して警告を出します。アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。wIPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

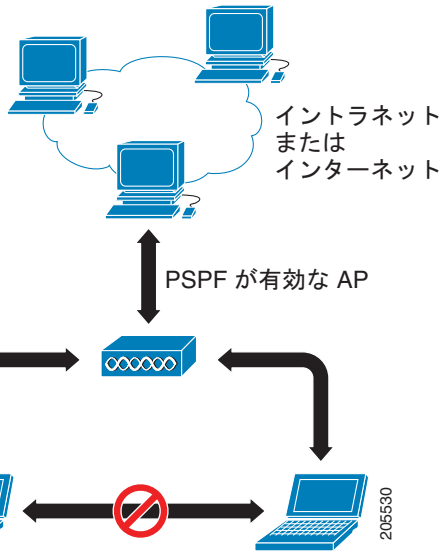
Publicly Secure Packet Forwarding（PSPF）違反の検出

アラームの説明と考えられる原因

Publicly Secure Packet Forwarding（PSPF）はワイヤレス クライアント同士の通信を無効にする機能であり、WLAN アクセス ポイントに実装されています。PSPF が有効になっている場合、ワイヤレス ネットワーク上のクライアント デバイス同士は通信できません。

ほとんどの WLAN 環境では、ワイヤレス クライアントは有線ネットワーク上の Web サーバなどのデバイスとだけ通信します。PSPF を有効にすると、ワイヤレス クライアントをワイヤレス侵入者によるハッキングから保護できます。PSPF は特に、空港、ホテル、喫茶店、大学構内など、認証がなく誰もがアクセス ポイントにアソシエートできるワイヤレス パブリック ネットワーク（ホットスポット）でワイヤレス クライアントを保護する場合に効果的です。PSPF 機能により、クライアント デバイスが誤ってワイヤレス ネットワーク上の他のクライアント デバイスとファイルを共有することが防止されます（図 A-18 を参照）。

図 A-18　ネットワーク上に有効になっている PSPF



ワイヤレス クライアント間でのワイヤレス トラフィックは許可しない

wIPS による解決

wIPS は、PSPF 違反を検出します。ワイヤレス クライアントが別のワイヤレス クライアントと通信しようとすると、wIPS は侵入攻撃の可能性に関するアラームを生成します。WLAN にワイヤレス プリンタまたは VoWLAN アプリケーションを導入している場合、このようなアプリケーションはクライアント間ワイヤレス通信を利用するため、このアラームは適用されません。

潜在的な ASLEAP 攻撃の検出

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは、WEP キー クラッキング攻撃に対して脆弱です（詳細については『*Weaknesses in the Key Scheduling Algorithm of RC4-I*』（Scott Fluhrer、Itsik Mantin、Adi Shamir 著）を参照）。

シスコは、既存の 802.1x フレームワークを利用して WEP キー攻撃を回避する LEAP（Lightweight Extensible Authentication Protocol）を導入しました。Cisco LEAP ソリューションには、セッションごとまたはユーザ キーに基づいて動的な相互認証と設定可能な WEP セッション キー タイムアウトが含まれています。LEAP ソリューションは安定したセキュリティ ソリューションとして見なされており、容易に設定できます。

LEAP を実行するワイヤレス LAN ネットワークを侵害するためオフライン辞書攻撃で LEAP パスワードを解読するハッキング ツールがあります。このツールは LEAP を採用している WLAN ネットワークを検出すると、ユーザを認証解除します。これによりユーザは再接続しなければならないため、ユーザ名とパスワードのクレデンシャルを入力します。ハッカーはネットワークへ再アクセスする正規ユーザのパケットをキャプチャします。その後攻撃者はトラフィックをオフラインで解析し、辞書の値をテストしてパスワードを推測できます。

ASLEAP ツールの主な機能を以下に示します。

- libpcap を使用して RFMON モードでワイヤレス インターフェイスからリアルタイムに読み取る。
- 1 つのチャネルをモニタするか、またはチャネル ホッピングを実行して LEAP を実行しているターゲット ネットワークを探す。

- LEAP ネットワークのユーザをアクティブに認証解除し、ユーザに再認証を実行させる。これにより LEAP パスワードを迅速にキャプチャできます。
- LEAP を実行していないユーザではなく、まだ確認されていないユーザのみを認証解除する。
- 保存されている libpcap ファイルを読み取る。
- ダイナミック データベース テーブルと索引を使用して大きなファイルを迅速に検索できるようにする。これにより、フラット ファイルの検索とは対照的に、最悪検索時間が .0015 % 短くなります。
- LEAP 交換情報のみを libpcap ファイルに書き込む。

これは、ディスク スペースが少ないデバイス（iPaq など）で LEAP クレデンシャルをキャプチャするときに使用できます。キャプチャされた LEAP クレデンシャルは、辞書攻撃を実行するためにそのデバイスよりもストレージ リソースが多いシステムの libpcap ファイルに保存されます。

このツールのソースと Win32 バイナリ ディストリビューションは http://asleap.sourceforge.net から入手できます。

シスコは、辞書攻撃を阻止する Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling（EAP-FAST）プロトコルを開発しました。EAP-FAST は中間者攻撃、辞書攻撃、パケットおよび認証偽造攻撃を阻止します。EAP-FAST では、クライアントとサーバ間に PAC（Protected Access Credential）を使用して相互認証するトンネルが作成されます。トンネル確立プロセスが完了したら、クライアントはユーザ名とパスワードのクレデンシャルを使用して認証されます。

EAP-FAST の特長には、次のものがあります。

- 独自のプロトコルではない。
- IEEE 802.11i 標準に準拠している。
- TKIP と WPA に対応している。
- 証明書を使用しないため複雑な PKI インフラストラクチャを回避する。
- PC および Pocket PC の複数のオペレーティング システムに対応している。

wIPS による解決

wIPS は、ASLEAP ツールの認証解除シグニチャを検出します。シグニチャを検出すると、サーバはワイヤレス管理者に警告します。攻撃を受けたステーションのユーザはパスワードをリセットする必要があります。最良の ASLEAP ツール対処策は、企業 WLAN 環境で LEAP を EAP-FAST に置き換える方法です。

NCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、弱い暗号化または認証を使用する設定されているアクセス ポイントを事前予防的に報告します。自動セキュリティ脆弱性スキャンの詳細については、NCS オンライン ヘルプを参照してください。

潜在的なハニーポット AP の検出

アラームの説明と考えられる原因

企業環境に WLAN を追加すると、ネットワーク セキュリティに対するまったく新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無認可のユーザに公開する可能性があります。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正アクセス ポイントの脅威以外にも、アクセス ポイントの設定ミスや未設定、DoS（サービス拒否）攻撃といったさまざまなワイヤレス セキュリティ リスクや侵入の可能性が存在します。

企業のワイヤレス ネットワークを対象とする最も効果的な攻撃の 1 つに、ハニー ポット アクセス ポイントを使用した攻撃があります。攻撃者は NetStumbler、Wellenreiter、MiniStumbler などのツールを使い、企業アクセス ポイントの SSID を検出します。次に建物の外（可能な場合は同じ建物の中）にアクセス ポイントをセットアップし、検出した企業 SSID をブロードキャストします。何も知らないクライアントが、信号強度が高いこのハニー ポット アクセス ポイントに接続します。アソシエートが完了すると、トラフィックがハニー ポット アクセス ポイントを経由するため、攻撃者はクライアント ステーションに対して攻撃を実行します。

wIPS による解決

wIPS によりハニー ポット アクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

ソフト AP またはホスト AP の検出

ホスト AP ツール：Cqure AP

アラームの説明と考えられる原因

ホストベースのアクセス ポイント（ワイヤレス アクセス スポットとして機能するデスクトップまたはラップトップ コンピュータ）は、企業のセキュリティに対する 2 つの脅威をもたらします。1 つ目の脅威は、ホストベース アクセス ポイントは一般に企業ワイヤレス インフラストラクチャに組み込まれておらず、企業のセキュリティ ポリシーに準拠しない不正なデバイスとなる可能性があることです。2 つ目の脅威は、ホストベースのアクセス ポイントは、ワイヤレス攻撃者によりさまざまな既知の攻撃（中間者攻撃、ハニーポット アクセス ポイント攻撃、アクセス ポイント偽装攻撃、DoS（サービス拒否）攻撃など）を実行するための便利なプラットフォームとして使用される点です。デスクトップまたはラップトップをアクセス ポイントとして設定するソフトウェア ツールはインターネットから簡単にダウンロードできるため、ホストベースのアクセス ポイントは単なる理論上の脅威の域を超えています。

一部のラップトップは、ホスト AP ソフトウェアがプリロードおよびアクティブにされた状態で出荷されます。このようなラップトップが企業ワイヤレス ネットワークに接続すると、ワイヤレス ネットワークがハッカーからの攻撃の危険性にさらされることになります。

wIPS による解決

wIPS が検出したソフト アクセス ポイントは、不正アクセス ポイントおよび侵入試行の可能性として処理する必要があります。wIPS によりソフト アクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

スプーフされた MAC アドレスの検出

スプーフィング ツールの一例：SMAC、macchanger、SirMACsAlot。

アラームの説明と考えられる原因

ワイヤレス攻撃者は、入手可能なさまざまな攻撃ツールを使ってワイヤレス ネットワークを妨害します。このようなツールの多くは、インターネットから無料でダウンロードできます。ほとんどのツールはスプーフされた MAC アドレスを利用します。スプーフされた MAC アドレスは、認可されたワイヤ

レス アクセス ポイントまたは認可されたクライアントとして動作します。攻撃者はこのようなツールを使ってさまざまな DoS（サービス拒否）攻撃を実行し、アクセス制御メカニズムを迂回し、ワイヤレス クライアントにサービスを不正にアドバタイズします。

wIPS による解決

wIPS はスプーフィングされた MAC アドレスを検出するため、IEEE 認可 OUI（ベンダー ID）と 802.11 フレーム シーケンス番号シグニチャを追跡します。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

疑わしい営業時間外のトラフィックの検出

アラームの説明と考えられる原因

ワイヤレス セキュリティ突破試行を検出する方法の 1 つに、ワイヤレス トラフィックが発生することにはなっていない時間とワイヤレス利用状況を照合する方法があります。wIPS サーバはこのアラームで設定された営業時間を基準にしてトラフィック パターンをモニタし、異常が検出されるとアラートを生成します。営業時間外に wIPS サーバにより追跡される疑わしいワイヤレス利用には、次のものがあります。

- セキュリティ侵害を示す可能性があるオフィス WLAN への認証要求またはアソシエート要求を発行するクライアント ステーション。
- ワイヤレス ネットワーク上での疑わしいダウンロードまたはアップロードを示す可能性があるワイヤレス データ トラフィック。

wIPS による解決

wIPS をグローバルに導入する場合、設定可能な営業時間範囲は現地時間で定義されます。管理を容易にするため、アクセス ポイントまたはセンサーを特定の時間帯に基づいて設定できます。オフィスと製造現場が混在する WLAN では、オフィスの WLAN SSID にオフィスの営業時間を定義し、製造現場の WLAN SSID に別の営業時間を定義できます。アラームが生成されたら、管理者は疑わしいトラフィックに関与するデバイスを特定してワイヤレス環境から削除してください。

ベンダー リストによる未承認アソシエーション

アラームの説明と考えられる原因

企業 WLAN 環境では、不正なステーションが原因でセキュリティの問題が発生し、ネットワーク パフォーマンスが低下します。このような不正なステーションは空間を占有し、ネットワーク帯域幅をめぐって競合します。アクセス ポイントが対応できるステーションの数は限られているため、アクセス ポイントは対応するステーションの数が上限に達すると、ステーションからのアソシエーション要求を拒否します。多数の不正なステーションに対応しており、これ以上のステーションに対応できないアクセス ポイントは、ネットワークにアクセスする正規のステーションを拒否します。不正なステーションによってよく引き起こされる問題には、接続の問題やパフォーマンス低下があります。

wIPS による解決

wIPS により、ネットワーク管理者は、ベンダー情報をポリシー プロファイルに含め、WLAN で使用中の未承認のベンダー製品であるステーションを効率的に検出できます。アラームが生成されます。

このアラームが生成されたら、未承認ステーションを特定し、この問題を解決するための措置をとる必要があります。この措置の 1 つに、不正の封じ込め処理を使用してブロックする方法があります。

未承認アソシエーションの検出

アラームの説明と考えられる原因

通常、企業ネットワーク環境では従業員が導入した不正なアクセス ポイントはネットワークの標準導入プラクティスに従っておらず、ネットワークの整合性を侵害します。このような不正なアクセス ポイントはネットワーク セキュリティの抜け穴であり、侵入者はこのアクセス ポイントからが企業の有線ネットワークに容易にハッキングできるようになります。多くのワイヤレス ネットワーク管理者が抱える主な課題の 1 つに、ACL に登録されているステーションと不正なアクセス ポイントの間の未承認アソシエーションがあります。ステーションと不正なアクセス ポイントの間でデータが転送されるため、ハッカーが機密情報を盗み出すことが可能になります。

不正なステーションはセキュリティの問題を引き起こし、ネットワーク パフォーマンスを低下させます。このような不正なステーションは空間を占有し、ネットワーク帯域幅をめぐって競合します。アクセス ポイントは一定の数のステーションにのみ対応できるため、アクセス ポイントは対応するステーションの数が上限に達すると、ステーションからのアソシエーション要求を拒否します。多数の不正なステーションに対応しており、これ以上のステーションに対応できないアクセス ポイントは、ネットワークにアクセスする正規のステーションを拒否します。不正なステーションによってよく引き起こされる問題には、接続の妨害やパフォーマンス低下があります。

wIPS による解決

アクセス ポイントとステーション間の未承認アソシエーションがネットワーク上で検出されると、wIPS はネットワーク管理者に対してこのアラームで通知します。このアラームが生成されたら、不正なデバイスまたは認可されていないデバイスを特定し、報告された問題を解決するための措置をとる必要があります。

Wellenreiter の検出

アラームの説明と考えられる原因

wIPS は、Wellenreiter ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。

Wellenreiter は、ウォードライビングとウォーチョーキングによく利用されるツールです。ワイヤレス ハッカーがウォードライビング ツールを使用してアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、ハッカーが車ではなく徒歩で徘徊します。ウォーウォーカーは、Wellenreiter や類似製品を使ってショッピングセンターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています。

このツールは、Prism2、Lucent、およびシスコ ベースのカードに対応しています。このツールは SSID と WEP 機能をブロードキャストしているインフラストラクチャとアドホック ネットワークを検出し、ベンダー情報を自動的に提供することができます。また、ethereal/tcpdump 互換ダンプ ファイルとアプリケーション savefile を作成します。GPS にも対応しています。ユーザは http://wellenreiter.sourceforge.net/index.html からこのツールをダウンロードできます。

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。wIPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

NCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、SSID をブロードキャストするように設定されているアクセス ポイントをすべて報告します。自動セキュリティ脆弱性スキャンの詳細については、NCS オンライン ヘルプを参照してください。

WiFiTap ツールの検出

アラームの説明と考えられる原因

WiFiTap ツールを使用すると、ワイヤレス攻撃者は、企業 AP に接続せずに、他のクライアントと直接通信するようにクライアントを設定できます。この実装により、攻撃者は、企業ネットワークに設定されているセキュリティ対策をすべて迂回して、個別のクライアントに攻撃することができます。これで、攻撃者は犠牲者のクライアント ステーションに保存されているすべてのファイルと情報にアクセスできます。

wIPS による解決

wIPS サーバは、WiFiTap ツールの使用をモニタして、使用を検出した場合にアラームを生成します。ユーザは、攻撃しているデバイスを特定し、ワイヤレス環境から取り除く必要があります。

APPENDIX B

不正アクセス ポイントの管理

この付録では、不正アクセス ポイントのセキュリティ問題とソリューションについて説明します。

この付録の構成は、次のとおりです。

不正アクセス ポイントの問題

不正アクセス ポイントは、正規のクライアントをハイジャックし、プレーン テキストまたは他の DoS 攻撃や中間者攻撃を使用することによって、無線 LAN の運用を妨害します。つまり、ハッカーは不正アクセス ポイントを使用して、パスワードやユーザ名などの機密情報を取得できるのです。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。このフレームはアクセス ポイントを模倣し、特定の無線 LAN クライアント アダプタに伝送して、他のすべてのアダプタには待機するように指示します。その結果、正規のクライアントは、無線 LAN リソースに接続できなくなります。したがって、無線 LAN サービス プロバイダーは、空間からの不正アクセス ポイントの締め出しに強い関心を持っています。

オペレーティング システムのセキュリティ ソリューションでは、「不正アクセス ポイントのロケーション、タギング、および封じ込め」（P.B-1）の説明にあるように、Radio Resource Management（RRM; 無線リソース管理）機能を使用して、すべての近隣アクセス ポイントを継続的にモニタし、不正アクセス ポイントを自動的に検出し、位置を特定します。

不正アクセス ポイントのロケーション、タギング、および封じ込め

NCS を使用して Cisco Unified Wireless Network Solution をモニタしている場合、不正アクセス ポイントが検出されるとフラグが生成され、既知の不正アクセス ポイントの MAC アドレスが表示されます。オペレータは、それぞれの不正アクセス ポイントに最も近いアクセス ポイントの場所を示すマップを表示できます。その後、それらを Known または Acknowledged 不正アクセス ポイントとしてマークする（追加の処置はなし）、それらを Alert 不正アクセス ポイントとしてマークする（監視し、アクティブになったときに通知）、それらを Contained 不正アクセス ポイントとしてマークする（1 ～ 4 台

のアクセス ポイントから、不正アクセス ポイントのクライアントが不正アクセス ポイントとアソシエートするたびにそれらのクライアントに認証解除とアソシエート解除のメッセージを送信することによって封じ込め処理を行う）のいずれかを実行します。

この組み込み型の検出、タギング、モニタリング、および封じ込めの機能を使用すると、システム管理者は、次に挙げる適切な処理を実行できます。

- 不正アクセス ポイントを特定します。
- 新しい不正アクセス ポイントの通知を受け取ります（通路をスキャンして歩く必要なし）。
- 不明な不正アクセス ポイントが削除または認識されるまでモニタします。
- 最も近い場所の認可済みアクセス ポイントを特定して、高速かつ効果的に誘導スキャンを行えるようにします。
- 1 ～ 4 台のアクセス ポイントから、不正アクセス ポイントのクライアントに認証解除とアソシエーション解除のメッセージを送信して、不正アクセス ポイントを封じ込めます。この封じ込め処理は、MAC アドレスを使って個々の不正アクセス ポイントに対して行うことも、企業サブネットに接続されているすべての不正アクセス ポイントに対して要求することもできます。
- 不正アクセス ポイントにタグを付けます。
  - 不正アクセス ポイントが LAN の外部にあり、LAN または無線 LAN のセキュリティを脅かさない場合は承諾します。
  - 不正アクセス ポイントが LAN または無線 LAN のセキュリティを脅かさない場合は容認します。
  - 不正アクセス ポイントが削除または認識されるまで、未知（管理対象外）のアクセス ポイントとしてタグ付けします。
  - 不正アクセス ポイントを封じ込め処理済みとしてタグ付けし、1 ～ 4 台のアクセス ポイントから、すべての不正アクセス ポイント クライアントに認証解除およびアソシエーション解除のメッセージを転送することにより、クライアントが不正アクセス ポイントにアソシエートしないようにします。この機能は、同じ不正アクセス ポイント上のすべてのアクティブなチャネルに適用されます。

不正アクセス ポイントの検出と特定

無線 LAN 上のアクセス ポイントの電源が入りコントローラにアソシエートされると、NCS はすぐに不正アクセス ポイントのリスニングを開始します。コントローラによって不正アクセス ポイントが検出されると、すぐに NCS に通知され、NCS によって不正アクセス ポイントのアラームが作成されます。

NCS が不正アクセス ポイント メッセージをコントローラから受け取ると、すべての NCS ユーザ インターフェイス ページの左下隅にアラーム モニタが表示されます。

不正アクセス ポイントを検出して特定するには、次の手順を実行します。

ステップ 1　[Rogues] インジケータをクリックして、[Rogue AP Alarms] ページを表示します。このページには、アラームの重大度、不正アクセス ポイントの MAC アドレス、不正アクセス ポイントのタイプ、不正アクセス ポイントが最初に検出された日時、および SSID が表示されます。

ステップ 2　[Rogue MAC Address] のリンクをクリックして、それに関連付けられた [Alarms > Rogue - AP MAC Address] ページを表示します。このページには、不正アクセス ポイントのアラームに関する詳細情報が表示されます。

ステップ 3　アラームを変更するには、[Select a command] ドロップダウン リストから次のコマンドのいずれかを選択し、[Go] をクリックします。

- [Assign to me]：選択されたアラームを現在のユーザに割り当てます。
- [Unassign]：選択されたアラームの割り当てを解除します。
- [Delete]：選択されたアラームを削除します。
- [Clear]：選択されたアラームをクリアします。
- [Event History]：不正アラームのイベントを表示できます。
- [Detecting APs]（無線帯域、場所、SSID、チャネル番号、WEP 状態、短いプリアンブルまたは長いプリアンブル、RSSI、および SNR を含む）：不正アクセス ポイントを現在検出しているアクセス ポイントを表示できます。
- [Rogue Clients]：この不正アクセス ポイントとアソシエートしているクライアントを表示できます。
- [Set State to 'Unknown - Alert']：不正アクセス ポイントを最も低い脅威としてタグ付けして不正アクセス ポイントの監視を継続し、封じ込め機能をオフにします。

  [Set State to 'Known - Internal']：不正アクセス ポイントを内部としてタグ付けして既知の不正アクセス ポイント リストに追加し、封じ込め機能をオフにします。

  [Set State to 'Known - External']：不正アクセス ポイントを外部としてタグ付けして既知の不正アクセス ポイント リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment] ～ [4 AP Containment]：level 1 containment を選択した場合は、不正な機器の近辺にある 1 つのアクセス ポイントが、その不正な機器にアソシエートされたクライアント デバイスに認証解除とアソシエート解除のメッセージを送信します。level 2 containment を選択した場合は、不正な機器の近辺にある 2 つのアクセス ポイントが、その不正な機器のクライアントに認証解除とディスアソシエーションのメッセージを送信します。この動作は level 4 まで同様です。

ステップ 4　[Select a command] ドロップダウン リストから [Map (High Resolution)] を選択して、[Go] をクリックします。[Maps > Building Name > Floor Name] ページに、計算された不正アクセス ポイントの現在位置が表示されます。

NCS Location を使用している場合は、複数のアクセス ポイントからの RSSI 信号強度を比較することによって、不正アクセス ポイントが存在する可能性が最も高い位置が特定され、その位置に小さなドクロと交差した 2 本の骨の形のインジケータが表示されます。アクセス ポイント 1 つと全方向性アンテナ 1 つだけの低展開ネットワークの場合、不正アクセス ポイントが存在する可能性が最も高い位置はアクセス ポイント周辺のリング上のいずれかの位置です。ただし、存在する可能性が高い位置の中心はアクセス ポイントとなります。NCS Base を使用している場合は、不正アクセス ポイントからの RSSI 信号強度を頼りに、不正な機器から最も強力な RSSI 信号を受信しているアクセス ポイントの隣に小さなドクロと交差した 2 本の骨の形のインジケータが表示されます。

アラームのモニタリング

この項では、次のトピックを扱います。

不正アクセス ポイントに関するアラームの監視

不正アクセス ポイント無線は、Cisco Lightweight アクセス ポイントによって検出された未許可のアクセス ポイントです。このページには、[Alarm Monitor] でクリックした重大度に基づいて、不正アクセス ポイントのアラームが表示されます。

[Rogue AP Alarms] ページを表示する手順は、次のとおりです。

- [Monitor] > [Alarms] の順に選択します。[Search] をクリックし、[Alarm Category] ドロップダウン リストから [Rogue AP] を選択します。[Go] をクリックして、該当するアラームを表示します。
- [Monitor] > [Security] の順に選択します。左側のサイドバーから、[Rouge AP] を選択します。
- 左側のサイドバー メニューの [Alarm Summary] ボックスで、[Malicious AP] の件数のリンクをクリックします。

（注） アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

表 B-1 に、[Rogue Access Point Alarms] ページに表示されるパラメータの説明を示します。

表 B-1　アラーム パラメータ

パラメータ	説明
Check box	操作対象となるアラームを選択します。
Severity	アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
Rogue MAC Address	不正アクセス ポイントの Media Access Control（MAC; メディア アクセス コントロール）アドレス。[Monitor Alarms] > [Rogue AP Details] を参照。
Vendor	不正アクセス ポイントのベンダー名、または Unknown（不明）。
Classification Type	Malicious（危険性あり）、Friendly（危険性なし）、Unclassified（未分類）。
Radio Type	この不正アクセス ポイントの無線タイプ。
Strongest AP RSSI	受信信号強度インジケータの最大値（dBm）。
No. of Rogue Clients	このアクセス ポイントにアソシエートされている不正クライアントの数。
Owner	不正アクセス ポイントの「オーナー」。
Date/Time	アラームの発生時刻。
State	State of the alarm：Alert（アラート）、Known（既知）、または Removed（削除済み）。
SSID	不正アクセス ポイント無線によってブロードキャストされている Service Set Identifier（SSID; サービス セット ID）。SSID がブロードキャストされない場合は空欄になります。
Map Location	この不正アクセス ポイントのマップ位置。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。

（注） アラームは NCS に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

[Rogue AP Alarms] ページには、次の追加フィールドがあります。

- [Unacknowledge] : すでに認知しているアラームを未認知にします。
- [E-mail Notification] : [All Alarms] > [E-mail Notification] ページへ移動し、電子メール通知を表示および設定できるようになります。詳細は、[Monitor Alarms] > [E-mail Notification] を参照してください。
- [Severity Configuration] : 新しく生成されたアラームの重大度を変更します。詳細は、[Monitor Alarms] > [Severity Configuration] を参照してください。
- [Detecting APs] : 現在、不正アクセス ポイントを検出している Cisco Lightweight アクセス ポイントを表示します。
- [Map (High Resolution)] : ここをクリックすると、不正アクセス ポイントの位置を示す高解像度マップが表示されます。
- [Rogue Clients] : ここをクリックすると、この不正アクセス ポイントにアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アクセス ポイントが表示されます。
- [Set State to 'Unclassified - Alert'] : このコマンドを選択して、不正アクセス ポイントを最も低い脅威としてタグ付けして不正アクセス ポイントの監視を継続し、封じ込め機能をオフにします。
- [Set State to 'Malicious - Alert'] : このコマンドを選択して、不正アクセス ポイントを「危険性あり」としてタグ付けします。
- [Set State to 'Friendly - Internal'] : このコマンドを選択して、不正アクセス ポイントを内部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment] : 不正アクセス ポイントを 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment] : 不正アクセス ポイントを 2 つの Cisco Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment] : 不正アクセス ポイントを 3 つの Cisco Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment] : 不正アクセス ポイントを 4 つの Cisco Lightweight アクセス ポイントで封じ込めます （最大封じ込めレベル）。

注意 不正アクセス ポイントの阻止は法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences. Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

不正アクセス ポイントの詳細な監視情報

[Rogue AP Alarms] ページでは、各不正アクセス ポイントに関するアラーム イベントの詳細を確認できます。

不正アクセス ポイント無線のアラーム イベントを確認するには、[Rogue AP Alarms] ページで [Rogue MAC Address] の下にある項目をクリックします。

このページには、不正アクセス ポイント無線のアラーム イベントが表示されます。不正アクセス ポイント無線は、Cisco Lightweight アクセス ポイントによって検出された未許可のアクセス ポイントです。表示される情報は次のとおりです。

- [General Info] :
  - [Rogue MAC Address]：不正アクセス ポイントの MAC アドレス。
  - [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
  - [On Network]：不正アクセス ポイントがネットワーク上にあるかどうかを示します。
  - [Owner]：オーナー（または空白）。
  - [Acknowledged]：担当ユーザがこのアラームを認知しているかどうかを示します。
  - [Classification Type]：Malicious、Friendly、Unclassified。
  - [State]：Alert（アラート）、Known（既知）、または Removed（削除済み）のアラームの状態を示します。
  - [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
  - [Channel Number]：不正アクセス ポイントのチャネル。
  - [Containment Level]：不正アクセス ポイントの封じ込めレベル、または Unassigned（未割り当て）。
  - [Radio Type]：この不正アクセス ポイントの無線タイプ。
  - [Strongest AP RSSI]：受信信号強度インジケータの最大値（dBm）。
  - [No. of Rogue Clients]：このアクセス ポイントにアソシエートされている不正クライアントの数。
  - [Created]：アラーム イベントが作成された日時。
  - [Modified]：アラーム イベントが修正された日時。
  - [Generated By]：アラーム イベントの生成元。
  - [Severity]：アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
  - [Previous Severity]：アラームの以前の重大度：Critical、Major、Minor、Clear が色分けして表示されます。
- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。
- [Message]：アラームに関する説明が表示されます。
- [Help]：アラームに関する最新情報が表示されます。
- [Event History]：ここをクリックすると、[Monitor Alarms > Events] ページが開きます。
- [Annotations]：このアラームの現在の注釈が表示されます。

ネットワーク上のアクセス ポイントの検出

不正アクセス ポイントを検出している Cisco Lightweight アクセス ポイントに関する情報を表示するには、アクセス ポイントの検出機能を使用します。

[Rogue AP Alarms] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Rogue AP Alarms] ページを表示するには、次のいずれかを実行します。

- 不正 AP の検索を実行します。この検索機能の詳細については、「Using the Search Feature」（P.2-34）を参照してください。
- NCS ホームページで、[Security] ダッシュボードをクリックします。このダッシュボードには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- [Alarm Summary] ボックスの [Malicious AP] の件数のリンクをクリックします。

ステップ 2　[Rogue AP Alarms] ページで、該当する不正アクセス ポイントの [Rogue MAC Address] をクリックします。[Rogue AP Alarms] 詳細ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Detecting AP on Network] を選択します。

ステップ 4　[Go] をクリックします。

いずれかのリスト項目をクリックすると、その項目に関するデータが表示されます。

- AP Name
- Radio
- Map Location
- Detecting AP Location
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [WEP]：有効または無効。
- [WPA]：有効または無効。
- [Pre-Amble]：Long（長型）または Short（短型）。
- [RSSI]：受信信号強度インジケータ（dBm）。
- [SNR]：信号対雑音比。
- [Containment Type]：このアクセス ポイントによる封じ込め処理のタイプ。
- [Containment Channels]：このアクセス ポイントが現在封じ込め処理を実行しているチャネル。

不正アドホック無線に関するアラームの監視

[Rogue Adhoc Alarms] ページには、不正アドホック無線のアラーム イベントが表示されます。

[Rogue Adhoc Alarms] ページを表示する手順は、次のとおりです。

- [Monitor] > [Alarms] の順に選択します。左側のサイドバー メニューで [New Search] を選択し、[Alarm Category] ドロップダウン リストから [Rogue Adhoc] を選択します。[Go] をクリックして、該当するアラームを表示します。
- [Monitor] > [Security] の順に選択します。左側のサイドバー メニューで、[Rogue Adhocs] を選択します。

（注）　アラーム ページが複数ある場合は、ページ上部にページ番号とその両側に他のページへ移動するためのスクロール矢印が表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

表 B-2 に、[Rogue Ad hoc Alarms] ページに表示されるフィールドの説明を示します。

表 B-2　不正アドホック無線のアラーム

パラメータ	説明
Check box	操作対象となるアラームを選択します。
Severity	アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
Rogue Adhoc MAC Address	不正アドホック無線デバイスの MAC アドレス。
Vendor	不正アドホック無線デバイスのベンダー名、または Unknown（不明）。
Classification Type	Malicious（危険性あり）、Friendly（危険性なし）、Unclassified（未分類）。
Radio Type	この不正アドホック無線の種類。
Strongest AP RSSI	受信信号強度インジケータの最大値（dBm）。
No.of Rogue Clients	この不正アドホック無線にアソシエートされている不正クライアントの数。
Owner	不正アドホック無線の「オーナー」。
Date/Time	アラームの発生時刻。
State	State of the alarm：Alert（アラート）、Known（既知）、または Removed（削除済み）。
SSID	不正アドホック無線によってブロードキャストされている Service Set Identifier。（SSID がブロードキャストされない場合は空欄になります）。
Map Location	この不正アドホック無線のマップ位置。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。

Select a Command

対応するチェックボックスを選択して 1 つ以上のアラームを選択し、[Select a command] ドロップダウン リストから次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択されたアラームをクリアします。
- [Clear]：選択されたアラームをクリアします。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。

（注）　アラームは NCS に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Detecting APs]：不正なアドホックを現在検出している Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントを表示します。詳細については、ネットワーク上のアクセス ポイントの検出を参照してください。

- [Map (High Resolution)]：ここをクリックすると、不正アドホック無線の位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、この不正アドホック無線にアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アドホック無線が表示されます。
- [Set State to 'Alert']：このコマンドを選択して、不正アドホック無線を最も低い脅威としてタグ付けして不正アクセス ポイントの監視を継続し、封じ込め機能をオフにします。
- [Set State to 'Internal']：このコマンドを選択して、不正アドホック無線を内部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [Set State to 'External']：このコマンドを選択して、不正アドホック無線を外部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment]：不正アドホック無線を 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アドホック無線を 2 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アドホック無線を 3 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アドホック無線を 4 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

注意　不正 AP の阻止は法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences.Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

不正アドホック無線に関する詳細の監視

[Rogue Adhoc Alarms] ページでは、各不正アドホック無線に関するアラーム イベントの詳細を確認できます。

不正アドホック無線のアラーム イベントを確認するには、[Rogue Adhoc Alarms] ページで [Rogue MAC Address] の下にある項目をクリックします。

このページには、不正アクセス ポイント無線のアラーム イベントが表示されます。不正アクセス ポイント無線は、Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントによって検出された無認可のアクセス ポイントです。表示される情報は次のとおりです。

- General:
  - [Rogue MAC Address]：不正アドホック無線デバイスの MAC アドレス。
  - [Vendor]：不正アドホック無線デバイスのベンダー名、または Unknown（不明）。
  - [On Network]：不正アドホック無線デバイスがネットワーク上にあるかどうかを示します。
  - [Owner]：オーナー（または空白）。
  - [Acknowledged]：担当ユーザがこのアラームを認知しているかどうかを示します。
  - [Classification Type]：Malicious、Friendly、Unclassified。
  - [State]：Alert（アラート）、Known（既知）、または Removed（削除済み）のアラームの状態を示します。

  - [SSID]：不正アドホック無線によってブロードキャストされている Service Set Identifier。（SSID がブロードキャストされない場合は空欄になります）。
  - [Channel Number]：不正アドホック無線のチャネル。
  - [Containment Level]：不正アドホック無線の封じ込めレベル、または Unassigned（未割り当て）。
  - [Radio Type]：この不正アドホック無線の種類。
  - [Strongest AP RSSI]：受信信号強度インジケータの最大値（dBm）。
  - [No.of Rogue Clients]：このアドホック無線にアソシエートされている不正クライアントの数を示します。
  - [Created]：アラーム イベントが作成された日時。
  - [Modified]：アラーム イベントが修正された日時。
  - [Generated By]：アラーム イベントの生成元。
  - [Severity]：アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
  - [Previous Severity]：アラームの以前の重大度：Critical、Major、Minor、Clear が色分けして表示されます。
- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。
- [Message]：アラームに関する説明が表示されます。
- [Help]：アラームに関する最新情報が表示されます。
- [Event History]：ここをクリックすると、[イベントのモニタリング] ページが開きます。
- [Annotations]：このアラームの現在の注釈が表示されます。

Select a Command

対応するチェックボックスを選択して 1 つ以上のアラームを選択し、次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択されたアラームを現在のユーザに割り当てます。
- [Unassign]：選択されたアラームの割り当てを解除します。
- [Delete]：選択されたアラームを削除します。
- [Clear]：選択されたアラームをクリアします。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。アラームは NCS に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。
- [UnAcknowledge]：すでに認知しているアラームの認知を解除できます。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Detecting APs]：不正なアドホックを現在検出している Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントを表示します。詳細については、「ネットワーク上のアクセス ポイントの検出」（P.B-6）を参照してください。
- [Map (High Resolution)]：ここをクリックすると、不正アドホック無線の位置を示す高解像度マップが表示されます。

- [Rogue Clients]：ここをクリックすると、この不正アドホック無線にアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アドホック無線が表示されます。
- [Set State to 'Alert']：このコマンドを選択して、不正アドホック無線を最も低い脅威としてタグ付けして不正アドホック無線の監視を継続し、封じ込め機能をオフにします。
- [Set State to 'Internal']：このコマンドを選択して、不正アドホック無線を内部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [Set State to 'External']：このコマンドを選択して、不正アクセス ポイントを外部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment]：不正アドホック無線を 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アドホック無線を 2 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アドホック無線を 3 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アドホック無線を 4 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

イベントのモニタリング

[Alarm Monitor] にある [Rogues] アラーム枠をクリックし、[Rogue MAC Addresses] のリスト項目をクリックします。次に、[Select a command] ドロップダウン リストから [Event History] を選択して、[Go] をクリックします。このページが表示されます。

[Monitor] > [Alarms] の順に選択し、左側のサイドバー メニューで [New Search] を選択します。[Severity] > [All Severities] および [Alarm Category] > [Rogue AP] の順に選択して、[Go] をクリックします。[Monitor Alarms > failure object] ページが表示されます。[Rogue MAC Address] 列の項目をクリックして、[Monitor Alarms > Rogue AP Details] ページを開きます。[Select a command] ドロップダウン リストから [Event History] を選択して、[Go] をクリックします。このページが表示されます。

このページでは、不正アラーム イベントに関する情報を参照できます。これらのイベントは発生した順に一覧表示されます。

各列のタイトルをクリックすると、表示順序を変更することができます。

- [Severity]：イベントの重大度が色分けして表示されます。
- [Rogue MAC Address]：リスト項目をクリックすると、そのエントリに関する情報が表示されます。
- [Vendor]：不正アクセス ポイントの製造業者名。
- [Type]：AP（アクセス ポイント）または AD-HOC（アドホック）。
- [On Network]：不正アクセス ポイントが、アソシエートされているポートと同じサブネットにあるかどうか。
- [On 802.11a]：不正アクセス ポイントが 802.11a 帯でブロードキャストしているかどうか。
- [On 802.11b]：不正アクセス ポイントが 802.11b/802.11g 帯でブロードキャストしているかどうか。
- [Date/Time]：アラームの日時。
- [Classification Type]：Malicious、Friendly、Unclassified。

- [State]：アラームの状態。Alert（アラート）、Removed（削除済み）など。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。

不正クライアントの監視

[Monitor] > [Alarms] の順に選択し、左側のサイドバー メニューで [New Search] を選択します。[Severity] > [All Severities] および [Alarm Category] > [Rogue AP] の順に選択して、[Go] をクリックします。[Monitor Alarms > failure object] ページが表示されます。[Rogue MAC Address] 列の項目をクリックして、[Monitor Alarms > Rogue AP Details] ページを開きます。[Select a command] ドロップダウン リストから [Rogue Clients] を選択します。このページが表示されます。

このページでは、不正アクセス ポイントにアソシエートされているクライアントに関する情報を参照できます。

- [Client MAC Address]：不正アクセス ポイントのクライアントの MAC アドレス。
- [Last Heard]：シスコ アクセス ポイントが不正アクセス ポイントのクライアントを最後に検出した時刻。
- [Status]：不正アクセス ポイントのクライアントの状態。

コントローラの設定

この項では、次のトピックを扱います。

- 「不正ポリシーの設定」（P.B-12）
- 「不正 AP ルールの設定」（P.B-13）

不正ポリシーの設定

このページでは、不正アクセス ポイントのポリシーを設定できます。

[Rogue Policies] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Security] > [Rogue Policies] の順に選択します。

- [Rogue Location Discovery Protocol]：[Enabled]、[Disabled]。
- Rogue APs
  - [Expiration Timeout for Rogue AP Entries (seconds)]：1 ～ 3600 秒（デフォルトは 1200）。
- Rogue Clients
  - [Validate rogue clients against AAA (check box)]：[Enabled]、[Disabled]
  - [Detect and report ad hoc networks (check box)]：[Enabled]、[Disabled] コマンド ボタン。
- [Save]：クライアント除外ポリシーへの変更を保存して、前のページに戻ります。
- [Audit]：NCS 値を、コントローラで使用された値と比較します。

不正 AP ルールの設定

このページでは、現在の不正 AP ルールの表示と編集ができます。

[Rogue AP Rules] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Security] > [Rogue AP Rules] の順に選択します。[Rogue AP Rules] ページに、不正 AP ルール、ルール タイプ（[Malicious] または [Friendly]）、およびルールの順序が表示されます。

ステップ 4　ルールの詳細を表示または編集するには、不正 AP ルールを選択します。詳細については、「不正 AP ルールの設定」（P.B-14）を参照してください。

コントローラ テンプレートの設定

この項では、次のトピックを扱います。

不正ポリシーの設定

このページでは、コントローラに適用される（アクセス ポイントとクライアントに対する）不正ポリシー テンプレートを設定できます。

現在のテンプレート、テンプレートが適用されているコントローラ数を表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue Policies] の順に選択します。

新しい不正ポリシー テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates] の順に選択します。

ステップ 2　左側のサイドバー メニューから、[Security] > [Rogue Policies] の順に選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Template] を選択します。

ステップ 4　[Go] をクリックします。

（注）　既存の不正ポリシー テンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue Policies] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5　[Rogue Location Discovery Protocol] チェックボックスをオンにして、有効にします。Rogue Location Discovery Protocol（RLDP）では、企業の有線ネットワークへの不正な接続の有無を判断します。

（注）　RLDP が有効の場合、コントローラは管理対象のアクセス ポイントに対して、不正アクセス ポイントをアソシエートし、特殊なパケットをコントローラへ送信するよう指示します。コントローラがこのパケットを受信すると、不正アクセス ポイントが企業ネットワークに接続されます。この方法は、暗号化を有効にしていない不正アクセス ポイントに対して機能します。

ステップ 6　不正アクセス ポイント エントリの失効タイムアウトを秒単位で設定します。

ステップ 7　[Validate rogue clients against AAA] チェックボックスをオンにして、不正クライアントの AAA 検証を有効にします。

ステップ 8　[Detect and report Adhoc networks] チェックボックスをオンにして、アドホック ネットワーキングに参加している不正クライアントの検出とレポートを有効にします。

ステップ 9　次のいずれかのボタンをクリックします。

- [Save]：クリックして現在のテンプレートを保存します。
- [Apply to Controllers]:クリックして現在のテンプレートをコントローラに適用します。[Apply to Controllers] ページで該当するコントローラを選択し、[OK] をクリックします。
- [Delete]：クリックして現在のテンプレートを削除します。現在コントローラにそのテンプレートが適用されている場合は、[OK] をクリックして、テンプレートが適用されている選択したコントローラから、テンプレートを削除することを確定します。
- [Cancel]：クリックして現在のテンプレート作成または現在のテンプレートの変更をキャンセルします。

不正 AP ルールの設定

不正 AP ルールを使用すると、不正アクセス ポイントを自動的に分類するルールを定義できます。NCS は、不正アクセス ポイントの分類ルールをコントローラに適用します。これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントは無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

（注）　不正 AP ルールは、誤アラームを減らすのにも役立ちます。

現在の分類ルール テンプレート、ルールの種類、適用されているコントローラ数を表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rules] の順に選択します。

（注）　不正クラスには以下の種類があります。
[Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。
[Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
[Unclassified Rogue]：検出されたアクセス ポイントのうち、Malicious ルールまたは Friendly ルールに該当しないアクセス ポイント。

不正アクセス ポイントの新しい分類ルール テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates] の順に選択します。

ステップ 2　左側のサイドバー メニューから、[Security] > [Rogue AP Rules] の順に選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Classification Rule] を選択します。

ステップ 4　[Go] をクリックします。

（注）　既存の不正 AP ルールのテンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rules] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5　次のフィールドに入力します。

- General:
  - [Rule Name] : テキスト ボックスにルールの名前を入力します。
  - [Rule Type] : ドロップダウン リストから [Malicious] または [Friendly] を選択します。

（注）　[Malicious Rogue] : 検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。
[Friendly Rogue] : 既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。

  - [Match Type] : ドロップダウン リストから [Match All Conditions] または [Match Any Condition] を選択します。
- Malicious Rogue Classification Rule
  - [Open Authentication] : オープン認証を有効にするには、このチェックボックスをオンにします。
  - [Match Managed AP SSID] : 管理対象 AP SSID のルール条件との一致を有効にするには、このチェックボックスをオンにします。

（注）　管理対象 SSID は、WLAN に対して設定された SSID で、システムが既知のものです。

  - [Match User Configured SSID] : ユーザ設定の SSID のルール条件との一致を有効にするには、このチェックボックスをオンにします。

（注）　ユーザ設定の SSID は、手動で追加された SSID です。[Match User Configured SSID] テキスト ボックスに、ユーザ設定の SSID を（1 行に 1 つずつ）入力します。

  - [Minimum RSSI] : 最小 RSSI 閾値制限を有効にするには、このチェックボックスをオンにします。

（注）　テキスト ボックスに RSSI 閾値の最小レベル（dB 単位）を入力します。検出されたアクセス ポイントがここで指定した RSSI 閾値を超えていると、そのアクセス ポイントは悪意のあるものとして分類されます。

– [Time Duration]：時間制限を有効にするには、このチェックボックスをオンにします。

（注） テキスト ボックスに制限時間（秒単位）を入力します。検出されたアクセス ポイントが指定した制限時間よりも長く表示されているとき、そのアクセス ポイントは悪意のあるものとして分類されます。

– [Minimum Number Rogue Clients]：悪意のあるクライアントの最小数の制限を有効にするには、このチェックボックスをオンにします。

（注） 悪意のあるクライアントを許可する最小数を入力します。検出されたアクセス ポイントにアソシエートされたクライアントの数が指定した値以上になると、そのアクセス ポイントは悪意のあるものとして分類されます。

ステップ 6　次のいずれかのボタンをクリックします。

- [Save]：クリックして現在のテンプレートを保存します。
- [Apply to Controllers]:クリックして現在のテンプレートをコントローラに適用します。[Apply to Controllers] ページで該当するコントローラを選択し、[OK] をクリックします。
- [Delete]：クリックして現在のテンプレートを削除します。現在コントローラにそのテンプレートが適用されている場合は、[OK] をクリックして、テンプレートが適用されている選択したコントローラから、テンプレートを削除することを確定します。
- [Cancel]：クリックして現在のテンプレート作成または現在のテンプレートの変更をキャンセルします。

不正 AP ルール グループの設定

不正 AP ルール グループ テンプレートを使用すると、複数の不正 AP ルールをコントローラに統合できます。

現在の不正 AP ルール グループ テンプレートを表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rule Groups] の順に選択します。

新しい不正 AP ルール グループ テンプレートを作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates] の順に選択します。

ステップ 2　左側のサイドバー メニューから、[Security] > [Rogue AP Rule Groups] の順に選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Rogue Rule Group] を選択します。

ステップ 4　[Go] をクリックします。

（注） 既存の不正ポリシー テンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rule Groups] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5　次のパラメータを入力します。

- General

– [Rule Group Name]：テキスト ボックスにルール グループの名前を入力します。

ステップ 6　Rogue AP ルールを追加するには、左の列のルールをクリックして強調表示します。[Add] をクリックして、強調表示したルールを右側の列に移動します。

（注）　不正 AP ルールは、[Rogue AP Rules] グループ ボックスから追加できます。詳細については、「不正 AP ルールの設定」（P.B-14）を参照してください。

ステップ 7　不正 AP ルールを削除するには、右の列のルールをクリックして強調表示します。[Remove] をクリックして、強調表示したルールを左側の列に移動します。

ステップ 8　[Move Up]/[Move Down] ボタンをクリックして、ルールが適用される順序を指定します。任意のルールを強調表示し、[Move Up] または [Move Down] をクリックして、現在のリストで上下に移動させます。

ステップ 9　不正 AP ルール リストを保存するには、[Save] をクリックします。

ステップ 10　現在のリストに変更を加えずにページを終了するには [Cancel] をクリックします。

（注）　コントローラに適用されたルールを表示または編集するには、[Configure] > [Controller] の順に選択し、コントローラ名をクリックしてコントローラを開きます。

APPENDIX C

無線リソース管理

オペレーティング システムのセキュリティ ソリューションでは、無線リソース管理（RRM）機能を使用して、すべての近隣アクセス ポイントを継続的にモニタし、不正アクセス ポイントを自動的に検出して特定します。

Cisco Unified Wireless Network に内蔵されている RRM は、RF 環境をモニタし、検出されたパフォーマンスの問題を動的に修正します。

この付録の構成は、次のとおりです。

RRM ダッシュボード

RRM は、ネットワークに追加された新しいコントローラや Lightweight アクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントは、使用国で有効なすべての 802.11a/b/g チャネルに加えて、他の地域で使用可能なチャネルも同時にスキャンできます。アクセス ポイントは、これらのチャネルのノイズや干渉をモニタする際、最大で 60 ミリ秒の間「オフチャネル」になります。不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

（注） 過去 100 ミリ秒間に音声トラフィックがある場合、アクセス ポイントはオフチャネル測定を延期し、チャネルは変更しません。

各アクセス ポイントがオフチャネルになるのはすべての時間のわずか 0.2% です。この動作はすべてのアクセス ポイントに分散されるので、隣接するアクセス ポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。そのため管理者は、すべてのアクセス ポイントを監視でき、ネットワークの可視性が向上します。

NCS により RRM 統計のスナップショットが提供されるので、障害のある場所、チャネルまたは電力レベルの変更について考えられる理由を特定することができます。ダッシュボードは、ネットワーク全体の RRM パフォーマンスの統計を示し、イベントのグループ化（アクセス ポイントのパフォーマンス、同一 RF グループのコントローラ間の設定の不一致、しきい値に基づいてアクセス ポイントによって検出されたカバレッジ ホール、最大電力で操作しているアクセス ポイントの割合など）に基づいてチャネルの変更を予測します。

（注）　RRM ダッシュボードの情報は、CAPWAP アクセス ポイントにだけ使用できます。

この項では、次のトピックを扱います。

チャネルの変更通知

同じチャネル上の 2 つの隣接するアクセス ポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突が発生すると、アクセス ポイントではデータがまったく受信されません。この機能は、たとえばカフェで E メールを読んでいるユーザが近隣ビジネスのアクセス ポイントのパフォーマンスに影響を与える場合に、問題となる場合があります。ネットワークが完全に分けられている場合でも、チャネル 1 のカフェにトラフィックを送信するユーザは、同じチャネルを使用する企業の通信を妨害する場合があります。コントローラは、アクセス ポイント チャネルを動的に割り当てて衝突を回避し、キャパシティとパフォーマンスを改善することで、この問題に対処します。チャネルは「再利用」され、希少な RF リソースが浪費されるのを防ぐことができます。つまり、チャネル 1 はカフェから離れた別のアクセス ポイントに割り当てられます。これは、チャネル 1 をまったく使用しない場合よりも効果的です。

コントローラの動的チャネル割り当て（DCA）機能は、アクセス ポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、1 や 2 など、802.11b/g 帯域の 2 つのオーバーラップするチャネルでは、両方が同時に 11/54 Mb/s を使用することはできません。コントローラは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離し、この問題を防ぎます。

チャネルに変更が行われると、NCS RRM ダッシュボードに通知が送信されます。チャネルの変更は、モードを [auto] または [on demand] に設定できる DCA 設定によって異なります。モードが [auto] の場合、この操作を許可するすべての CAPWAP アクセス ポイントに対し、チャネル割り当てが定期的に更新されます。モードが [on demand] に設定されている場合、要求に基づいてチャネル割り当てが更新されます。DCA が静的である場合、動的チャネル割り当ては行われず、値はグローバル デフォルトに設定されます。

DCA は、5 GHz 帯域で 802.11n 40 MHz チャネルをサポートします。40 MHz のチャネライゼーションを行うと、無線はより高い瞬間データ率に達することができます（20 MHz チャネルの約 2.25 倍）。DCA の稼働を 20 MHz または 40 MHz から選択できます。

（注）　2.4 GHz 帯域で 40 MHz のチャネライゼーションを使用する無線は、DCA ではサポートされません。

チャネル変更のトラップが受信され、チャネル変更が前に行われている場合、イベントは [Channel Revised] とマークされます。そうでない場合、[Channel Changed] とマークされます。チャネル変更の各イベントには、いくつかの理由があります。原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。たとえば、チャネル変更が信号、干渉、またはノイズによって発生するとします。原因コードが通知として受信されたときに、すべての原因を対象として原因コードの係数が変更されます。そのイベントの理由が 3 つある場合は、原因コードの係数は理由 1 つあたり 1/3 または 0.33 に変更されます。10 件のチャネル変更イベントが同じ原因コードで受信された場合、3 つの原因コードすべてに同じ係数が与えられて、チャネル変更の原因が判定されます。

送信電力変更通知

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。通常は、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。コントローラは、3 番目に伝送パワーの強いネイバーによるアクセス ポイントの認識に応じて、アクセス ポイントの送信電力を調整します。

送信電力コントロール アルゴリズムは、アクセス ポイントの電力のみ少なくします。ただし、カバレッジ ホール アルゴリズムを使用して、アクセス ポイントの電力を拡大し、カバレッジ ホールに対応します。たとえば、アクセス ポイントの障害が検出された場合、カバレッジ ホール アルゴリズムを使用して、周辺アクセス ポイント電力を自動的に拡大し、カバレッジの損失によって発生したギャップに対応できます。

送信電力に変更が行われると、NCS RRM ダッシュボードに通知が送信されます。送信電力変更の各イベントには、いくつかの理由があります。原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。

RF グループ化通知

RRM がコントローラに実行されると、動的グループ化が行われ、新しいグループ リーダーが選択されます。動的グループ化のモードは、オンとオフの 2 つです。グループ化をオフにすると、動的グループ化は行われなくなり、各スイッチは自身の CAPWAP アクセス ポイント パラメータだけを最適化します。グループ化をオンにすると、スイッチはグループを形成し、リーダーを選択してより適切な動的パラメータの最適化を実行します。グループ化をオンにすると設定した間隔（秒）はグループ化アルゴリズムが実行される期間を示します （グループ化アルゴリズムは、グループに変更があり、自動グループ化が有効である場合にも実行されます)。

RRM ダッシュボードの表示

RRM ダッシュボードにアクセスするには、[Monitor] > [RRM] の順に選択します。

RRM ダッシュボードには次の情報が表示されます。

- [RRM Statistics] には、ネットワーク全体の統計が表示されます。
- [Channel Change Reason] には、すべての 802.11a/b/g/n 無線のチャネルが変更した理由が表示されます。
- [Channel Change] には、完了したすべてのイベントが原因とともに表示されます。
- [Configuration Mismatch] には、リーダーとメンバーの比較が表示されます。
- [Coverage Hole] には、カバレッジ ホールの深刻さが評価され、その位置が表示されます。
- [Percent Time at Maximum Power] には、アクセス ポイントが最大電力に達した時間の割合が表示され、これらのアクセス ポイントを示します。

次の統計情報が表示されます。

- [Total Channel Changes]：チャネルが更新または変更されたかどうかに関係なく、802.11a/b/g/n 無線のチャネル変更数の合計。カウントは、24 時間および 7 日間の期間に分割されます。割合のリンクまたは [24-hour] 列の下にあるリンクをクリックすると、そのアクセス ポイントのみの詳細を示すページが表示されます。
- [Total Configuration Mismatches]：24 時間に検出された設定の不一致数の合計。
- [Total Coverage Hole Events]：24 時間および 7 日間のカバレッジ ホール イベント数の合計。

- [Number of RF Groups]：現在 NCS が管理している RF グループ数の合計。
- [Configuration Mismatch]：24 時間に発生した設定の不一致を RF グループごとにグループ リーダーの詳細とともに表示します。
- [Percent of APs at MAX Power]：802.11a/n 無線のアクセス ポイントの割合を、最大電力に達したすべてのアクセス ポイントの割合の合計として表示します。最大電力レベルはプリセットされ、アクセス ポイントの現在の最大電力を参照します。

（注）　最大電力は、RRM ダッシュボードの 3 つの領域に表示されます。この最大電力の部分には、現在の値が表示され、ポーリングされます。

- [Channel Change Causes]：802.11a/n 無線のグラフィック棒グラフ。グラフは、チャネル変更が行われた理由に基づいて作成されます。グラフは 2 つの部分に分割され、それぞれ 24 時間および 7 日間に発生するイベントを引き起こす理由の重み付けされた理由の割合を示します。チャネル変更の各イベントにはいくつかの理由があり、その重みはそれらの理由に均等に分けられます。ネット原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。
- [Channel Change APs]：チャネル変更の各イベントには、CAPWAP アクセス ポイントの MAC アドレスも表示されます。各理由コードについて、チャネル イベントの重み付き理由に基づいて 802.11a/n アクセス ポイントに発生したチャネル変更の多くが表示されます。カウントは、24 時間および 7 日間の期間に分割されます。
- [Coverage Hole Events APs]：カバレッジ ホール イベントをトリガーした IF Type 11 a/n によってフィルタ処理された上位 5 件のアクセス ポイントが表示されます。
- [Aggregated Percent Max Power APs]：カバレッジ ホールおよびイベントを調整するために最大電力で動作している 802.11a/n CAPWAP アクセス ポイントの割合の合計を示すグラフィカルな進捗状況グラフ。カウントは、24 時間および 7 日間の期間に分割されます。

（注）　この最大電力の部分には、最近 24 時間の値が表示され、ポーリング主導となります。電力は 15 分ごとに、または無線のパフォーマンスに設定されるとポーリングされます。

- [Percent Time at Maximum Power]：最大電力で動作している上位 5 件の 802.11a/n CAPWAP アクセス ポイントのリスト。

（注）　この最大電力の部分には、最近 24 時間の値が表示され、イベント ドリブンのみです。

コントローラの設定

この項では、次のトピックを扱います。

- 「RRM しきい値コントローラの設定（802.11a/n または 802.11b/g/n 用）」（P.C-4）
- 「40 MHz チャネル ボンディングの設定」（P.C-5）

RRM しきい値コントローラの設定（802.11a/n または 802.11b/g/n 用）

802.11a/n または 802.11b/g/n の RRM しきい値コントローラを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　該当するコントローラの [IP address] をクリックして、[Controller Properties] ページを開きます。

ステップ 3　左側のサイドバー メニューから [802.11a/n] > [RRM Thresholds] または [802.11b/g/n] > [RRM Thresholds] を選択します。

ステップ 4　[Coverage Level]、[Load Thresholds]、および [Threshold For Traps] に対して変更が必要な場合には、変更します。

（注）　[Coverage Thresholds Min SNR Level (dB)] パラメータを調整すると、[Signal Strength (dB)] の値が自動的にこの変更に反映されます。[Signal Strength (dB)] パラメータにより、SNR 値を調整する際のカバレッジのしきい値の対象範囲に関する情報が提供されます。

ステップ 5　[Save] をクリックします。

40 MHz チャネル ボンディングの設定

[Radio Resource Management (RRM) Dynamic Channel Assignment (DCA)] ページを使用して、このコントローラのチャネル幅のほか、DCA チャネルを選択できます。

RRM DCA は、5 GHz 帯域で 802.11n 40 MHz チャネルをサポートします。より高い帯域幅を使用すると、瞬間的データ レートが高くなります。

（注）　大きい帯域幅を選択すると、オーバーラッピングしないチャネルが減少するため、構成によってはネットワーク全体のスループットが低下することがあります。

各コントローラに 802.11 a/n RRM DCA チャネルを設定する手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [RRM DCA] の順に選択します。[802.11a/n RRM DCA] ページが表示されます。

（注）　[Configure] > [Access Points] の順に選択し、[Radio] 列で [802.11a/n] リンクをクリックして、アクセス ポイントのページでチャネル幅を設定することもできます。[Current RF Channel Assignment] が表示され、[Global] 割り当て方式を選択するか、[Custom] を選択してチャネルを指定できます。

ステップ 4　[Channel Width] ドロップダウン リストから、[20 MHz] または [40 MHz] を選択します。

（注）　20 MHz デバイスと 40 MHz デバイスが混在する展開の場合は注意が必要です。40 MHz デバイスのチャネル アクセス ルールは若干異なるため、20 MHz デバイスに悪影響を与える場合があります。

（注）　アクセス ポイントの無線のチャネル幅を表示するには、[Monitor] > [Access Points] > [<name>] > [Interfaces] タブの順に選択します。[Configure] > [Access Points] の順に選択し、[Radio] 列で該当する無線をクリックして、チャネル幅とアンテナの選択肢を表示することもできます。

ステップ 5　該当する DCA チャネルのチェックボックスを選択します。選択したチャネルが、[Selected DCA channels] テキスト ボックスに表示されます。

ステップ 6　[Save] をクリックします。

コントローラ テンプレートの設定

この項では、次のトピックを扱います。

RRM しきい値テンプレートの設定（802.11a/n または 802.11b/g/n 用）

新しい 802.11a/n または 802.11b/g/n RRM しきい値テンプレートを追加する、または既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates] の順に選択します。

ステップ 2　左側のサイドバー メニューから [802.11a/n] > [RRM Thresholds] または [802.11b/g/n] > [RRM Thresholds] を選択します。

ステップ 3　新しいテンプレートを追加するには、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、[Template Name] 列のテンプレート名をクリックします。802.11a/n または 802.11b/g/n RRM しきい値テンプレートのページが表示され、テンプレートが適用されるコントローラの数が自動的に読み込まれます。

ステップ 4　現在コントローラにアソシエートされている故障したクライアントの最小数を入力します。

ステップ 5　希望のカバレッジ レベルを入力します。測定されたカバレッジがカバレッジ例外レベルで設定された割合分減少した場合、カバレッジ ホールが生成されます。

ステップ 6　[Signal Strength (dB)] パラメータにより、カバレッジのしきい値の対象範囲を示します。

ステップ 7　現在コントローラにアソシエートされているクライアントの最大数を入力します。

ステップ 8　[RF Utilization] テキスト ボックスに、802.11a/n または 802.11b/g/n のしきい値のパーセンテージを入力します。

ステップ 9　干渉しきい値を入力します。

ステップ 10　ノイズ閾値を -127 ～ 0dBm の範囲で入力します。このしきい値を超えると、コントローラは NCS にアラームを送信します。

ステップ 11　カバレッジ例外レベルの割合を入力します。最小クライアント数に設定されたカバレッジから、この割合分減少した場合、カバレッジ ホールが生成されます。

ステップ 12　[Noise/Interference/Rogue Monitoring Channels] セクションの [Channel List] ドロップダウン リストから、必要なモニタリング レベルに基づいて、[all channels]、[country channels]、または [DCA channels] を選択します。動的チャネル割り当て（DCA）により、コントローラに接続された管理対象デバイスの中から妥当なチャネルの割り当てが自動的に選択されます。

ステップ 13　[Save] をクリックします。

RRM 間隔テンプレートの設定（802.11a/n または 802.11b/g/n 用）

802.11a/n または 802.11b/g/n RRM 間隔テンプレートを追加する、または既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates] の順に選択します。

ステップ 2　左側のサイドバー メニューから、[802.11b/g/n] > [RRM Intervals] を選択します。

ステップ 3　新しいテンプレートを追加するには、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、[Template Name] 列のテンプレート名をクリックします。

802.11a/n または 802.11b/g/n RRM しきい値テンプレートが表示され、テンプレートが適用されるコントローラの数が自動的に読み込まれます。

ステップ 4　各アクセス ポイントに対して強度測定を行う間隔を入力します。デフォルトは 300 秒です。

ステップ 5　各アクセス ポイントに対してノイズおよび干渉測定を行う間隔を入力します。デフォルトは 300 秒です。

ステップ 6　各アクセス ポイントに対して負荷測定を行う間隔を入力します。デフォルトは 300 秒です。

ステップ 7　各アクセス ポイントに対してカバレッジ測定を行う間隔を入力します。デフォルトは 300 秒です。

ステップ 8　[Save] をクリックします。

INDEX

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
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/