

## Cisco NAC

Cisco® NAC(ネットワーク アドミッション コントロール)ソリューションにより、ネットワーク管理者は、事前に有線、無線、およびリモートのユーザとマシンを認証し、権限の付与、評価、および修復を行ってから、そのユーザに対してネットワークへのアクセスを許可することができます。ネットワーク接続されたデバイス(ノート型パソコン、デスクトップ パソコン、その他の企業資産など)がセキュリティ ポリシーに適合しているかどうかを識別し、ネットワークへのアクセスを許可する前に脆弱性の修復を行います。

### 製品概要

Cisco NAC は、導入が容易なエンドツーエンドのネットワーク登録およびポリシー適用ソリューションです。この高度なネットワーク セキュリティ製品は、次の機能を備えています。

- ネットワーク内のユーザ、デバイス、およびそのロールを認識できます。この最初のステップは認証を行う時点で実行され、悪意あるコードによってダメージを受ける心配がありません。
- マシンがセキュリティ ポリシーに適合しているかどうかを評価します。セキュリティ ポリシーは、ユーザ タイプ、デバイス タイプ、または OS ごとに設定できます。
- セキュリティ ポリシーを適用し、適合していないマシンを遮断、隔離、および修復します。適合していないマシンは検疫エリアへ入れられ、管理者の判断に応じて修復されます。

Cisco NAC の導入により、次の条件に関係なく、すべてのデバイスに対してポストチャ評価および修復サービスを行うことができます。

- **デバイスのタイプ:** Cisco NAC を使用すると、Windows マシン、Mac マシン、Linux マシン、ノート型パソコン、デスクトップ パソコン、PDA、その他の企業資産(プリンタや IP フォン)など、すべてのネットワーク接続されたデバイスに対してセキュリティ ポリシーを適用できます。
- **デバイスの所有者:** Cisco NAC を使用すると、企業、社員、請負業者、およびゲストが所有するシステムにセキュリティ ポリシーを適用できます。
- **デバイスのアクセス方法:** Cisco NAC は、LAN、WLAN、WAN、または VPN 経由で接続するデバイスにネットワーク アドミッション コントロールを実施します。

Cisco NAC は、別の製品や追加モジュールを用意することなく、すべての運用シナリオに対してポリシーを適用可能な独自の機能を備えています。

### 機能と利点

Cisco NAC ソリューションは次のようなさまざまな方法で、企業に恩恵をもたらします。

- セキュリティ ポリシーを適用することにより、コンプライアンス要件に対応する
- 不正なネットワーク アクセスを防止し、貴重な情報資産を保護する
- ウイルス、ワーム、スパイウェア、およびその他の悪意あるアプリケーションなどのネットワークの脅威から、予防的に防御する
- 定期的に評価および修復することで、ユーザ マシンの脆弱性を最小限に抑える
- エンドポイント マシンの識別、トラッキング、修復および更新プロセスを自動化することで、大幅なコスト削減を達成する

### 認証の統合とシングル サインオン

Cisco NAC は、ほとんどの認証方式で認証プロキシとして機能します。Kerberos、Lightweight Directory Access Protocol (LDAP)、RADIUS、Active Directory、S/Ident などの認証方式と統合可能です。エンド ユーザの利便性を向上させるために、Cisco NAC では、VPN クライアント、無線クライアント、および Windows Active Directory ドメインのシングル サインオンをサポートしています。管理者はロールベースのアクセス コントロールを実行することで、さまざまな権限レベルの複数のユーザ プロファイルを維持できます。

### 脆弱性の評価

Cisco NAC は、すべての Windows、Mac OS、Linux ベースの OS およびマシン、そしてゲームコンソール、PDA、プリンタ、IP フォンなどの PC 以外のネットワーク接続されたデバイスのスキャンをサポートしています。NAC はネットワークベースのスキャンを実施しますが、必要に応じてカスタムビルトのスキャンを実施することもできます。Cisco NAC は、レジストリ キーの設定、稼働中のサービス、またはシステム ファイルによって特定されるすべてのアプリケーションをチェックできます。

### デバイスの検疫

Cisco NAC は、ポリシーに適合していないマシンを検疫エリアへ入れます。これによって、修復リソースへのマシンのアクセスを維持しながら、感染の拡大を防ぐことができます。検疫には、/30 程度のサイズの小さいサブネットを使用するか、検疫 VLAN を使用します。

### セキュリティ ポリシーの自動更新

標準ソフトウェア メンテナンス パッケージの一部としてシスコが提供するセキュリティ ポリシーの自動更新機能では、重要な OS の更新、アンチウイルス ソフトウェアのウイルス定義の更新、およびアンチスパイウェアの定義更新をチェックするポリシーを含め、一般的なネットワーク アクセス条件に関するポリシーが事前に設定されています。これにより、Cisco NAC によって常に最新のポリシーを維持できるため、ネットワーク管理者の管理コストが軽減します。

### 中央集中型の管理

管理者は、Cisco NAC の Web ベースの管理コンソールを使用して、ユーザが属するロールごとに必要なスキャンのタイプと、リカバリに必要な関連する修復パッケージを定義することができます。1 つの管理コンソールから複数のサーバを管理できます。

### 修復

検疫エリアに隔離されたデバイスには修復サーバへのアクセス権が与えられます。修復サーバは、OS のパッチとアップデート、ウイルス定義ファイル、または Cisco Security Agent などのエンドポイント セキュリティ ソリューションを提供することができます。管理者は、オプションのエージェントを使用して自動修復を有効にしたり、一連の修復手順を指定したりできます。また、Cisco NAC は監視モードやサイレント修復などの使いやすい機能を提供し、ユーザへの影響を最小にします。

### 柔軟な導入モード

Cisco NAC には、どんなネットワークにも対応できるよう幅広い導入モードが用意されています。仮想または実際の IP ゲートウェイとして、エッジまたは中央に配置できるほか、クライアントのレイヤ 2 またはレイヤ 3 アクセスに対応し、ネットワークトラフィックにインバンドまたはアウトオブバンドで導入できます。

### 導入モード

Cisco NAC は、お客様のネットワークに最適な方法で導入できます。表 1 に詳しい導入オプションを示します。

表 1 Cisco NAC の導入オプション

導入モデル	オプション
トラフィック通過モード	<ul style="list-style-type: none"> <li>仮想ゲートウェイ(ブリッジ モード)</li> <li>実際の IP ゲートウェイ/NAT ゲートウェイ(ルータ モード)</li> </ul>
物理的な導入モデル	<ul style="list-style-type: none"> <li>エッジ</li> <li>中央</li> </ul>
クライアント アクセス モード	<ul style="list-style-type: none"> <li>レイヤ 2(クライアントは Cisco NAC Server に隣接)</li> <li>レイヤ 3(クライアントは Cisco NAC Server から複数ホップ離して配置)</li> </ul>
トラフィック フロー モデル	<ul style="list-style-type: none"> <li>インバンド(Cisco NAC Server はユーザトラフィックに対して常にインライン)</li> <li>アウトオブバンド(Cisco NAC Server は、認証、ポスチャ評価、および修復の場合のみインライン)</li> </ul>

## 製品アーキテクチャ

Cisco NAC には、いくつかの中核的コンポーネントと、機能強化のための追加オプション コンポーネントがあります。

- Cisco NAC Server:** エンドポイントがポリシーに適合しているかどうかに基づいて、評価を開始し、アクセス権限を決定するデバイスです。ユーザは、ポート レイヤでブロックされ、検査に合格するまで、信頼されるネットワークへのアクセスは制限されます。Cisco NAC Server には、オンラインの同時ユーザ数(100、250、500、1,500、2,500、3,500 および 5,000 ユーザ)に基づいて、7 つのサイズが用意されています。1 つの会社で、サイズの異なる複数のサーバを使用することができます。たとえば、本社ビルで 1,500 ユーザの Cisco NAC Server を使用し、同じ会社のブランチ オフィスでは 100 ユーザのサーバを使用できます。
- Cisco NAC Manager:** ユーザのロール、チェック、ルール、およびポリシーを確立するための一元化された Web ベースのコンソールです。Cisco NAC Manager には 3 つのサイズが用意されています。Cisco NAC Lite Manager では、最大 3 台の Cisco NAC Server を管理できます。Cisco NAC Standard Manager では最大 20 台の Cisco NAC Server を管理でき、Cisco NAC Super Manager では最大 40 台の Cisco NAC Server または 80 台の Cisco NAC ネットワーク モジュールを管理できます。
- Cisco NAC Agent:** ポスチャ評価機能を拡張し、修復を効率化するコンパクトな読み取り専用のエージェントです。Cisco NAC Agent はオプションであり、無料で配布されます。

## その他の NAC サービス

中核をなす Cisco NAC Manager および Server のユーザ認証、デバイス準拠性評価、ロールベースのアクセス コントロールの機能に加え、いくつかの高度な Cisco NAC サービス オプションがさらなる運用上の利点とポリシー コントロールを提供します。

- Cisco NAC Profiler:** オプションの Cisco NAC Profiler は、IP フォンやプリンタ、スキャナなどの認証不要デバイスを含む、ネットワークに接続されたすべてのデバイスのリアルタイムのコンテキスト インベントリを維持することで、コンピュータ以外のデバイスのプロファイリングを提供します。Cisco NAC の展開と、エンドポイント デバイスの検出および追跡に関連する管理タスクを大幅に軽減します。Cisco NAC Profiler データシートは、[http://www.cisco.com/web/JP/product/hs/security/cca/prodlit/nacp\\_ds.html](http://www.cisco.com/web/JP/product/hs/security/cca/prodlit/nacp_ds.html) を参照してください。
- Cisco NAC ゲスト サーバ:** オプションの Cisco NAC ゲスト サーバは、有線および無線ネットワーク上のゲスト ユーザのプロビジョニング、通知、管理、レポートを簡略化し、会社の訪問者のサポートに関連する一般的な課題から IT スタッフを解放します。セキュアなゲスト サービスは、訪問者の業務上のニーズを満たすセキュアで柔軟なネットワーク アクセスを提供すると同時に、自社の資産、従業員、そして情報を保護するための IT 能力を強化します。Cisco NAC ゲス

トサーバのデータシート

は、[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product\\_data\\_sheet0900aecd806e98c9.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd806e98c9.html) [英語] を参照してください。

図 1 は、インバンド モードでの Cisco NAC を論理的に示した図です。この構成は、Cisco Aironet® アクセス ポイントを含むすべての 802.11 無線アクセス ポイントと連動して動作します。インバンド モードは、VPN トラフィックにも適した導入モードです。

図 1 インバンド モードでの Cisco NAC アーキテクチャ

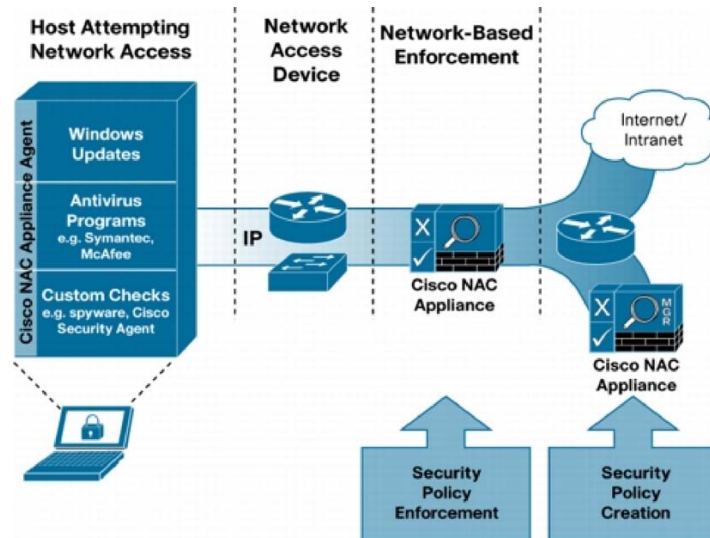
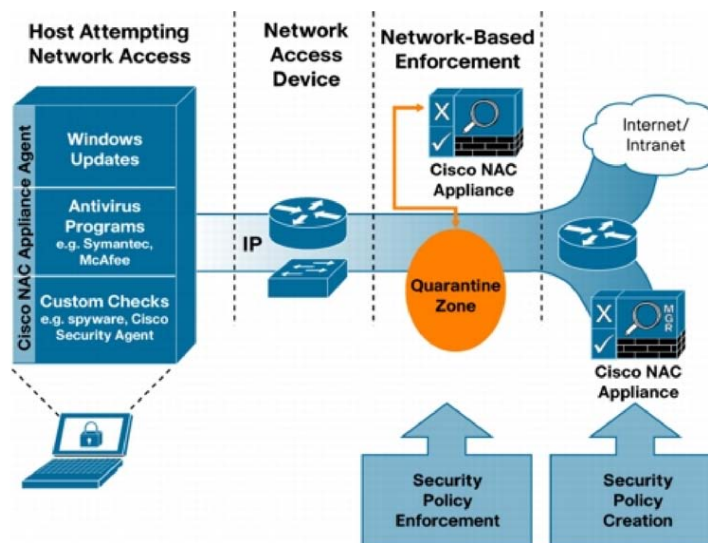


図 2 は、アウトオブバンド モードでの Cisco NAC を論理的に示した図です。このモードでは、Cisco NAC Server は、認証、ポスチャ評価、および修復の処理中だけインバンドとなります。ユーザのデバイスが正常にログオンしたあとは、そのデバイスのトラフィックはスイッチ ポートへ直接送られます。

図 2 アウトオブバンド モードでの Cisco NAC アーキテクチャ



トラフィックフローモードのほか、お客様のネットワークに最適な方法でNACを導入できるよう、多様な導入オプションがあります。表2に、その他の導入オプションの一覧を示します。

表2 Cisco NAC ネットワーク モジュール導入オプション

導入モデル	オプション
トラフィック通過モード	<ul style="list-style-type: none"> <li>仮想ゲートウェイ(ブリッジモード)</li> <li>実際のIPゲートウェイ(ルータモード)</li> </ul>
クライアントアクセスモード	<ul style="list-style-type: none"> <li>レイヤ2(クライアントはCisco NAC Serverに隣接)</li> <li>レイヤ3(クライアントはCisco NAC Serverから複数ホップ離して配置)</li> </ul>
トラフィックフローモデル	<ul style="list-style-type: none"> <li>インバンド(Cisco NAC Serverはユーザトラフィックに対して常にインライン)</li> <li>アウトオブバンド(Cisco NAC Serverは、認証、ポスチャ評価、および修復の場合のみインライン)</li> </ul>

インバンドモードのCisco NACはあらゆるネットワークインフラストラクチャに対応しますが、アウトオブバンドモードはSimple Network Management Protocol(SNMP; 簡易ネットワーク管理プロトコル)を使用してスイッチと通信します。対応しているスイッチの最新リストは、[http://www.cisco.com/en/US/docs/security/nac/appliance/support\\_guide/switch\\_spt.html](http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html) [英語]を参照してください。このリストは頻繁に更新されます。

### 製品仕様

NAC ServerおよびNAC Managerのベースとなる3つの新しいハードウェアオプションを用意しました。表3にCisco NACのハードウェアアプライアンスバージョンの仕様を示します。

表3 Cisco NAC アプライアンスのハードウェア仕様

	Cisco NAC Appliance 3315	Cisco NAC Appliance 3355	Cisco NAC Appliance 3395
製品	100, 250 および 500 ユーザ向けの Cisco NAC Server Cisco NAC Access Lite Manager	1500, 2500, 3500 および 5000 ユーザ向けの Cisco NAC Server Cisco NAC Standard Manager	Cisco NAC Super Manager
プロセッサ	クアッドコア Intel Xeon (Core 2 Quad)	クアッドコア Intel Xeon (Nehalem)	クアッドコア Intel Xeon (Nehalem) × 2
メモリ	4 GB	6 GB	8 GB
ハードディスク	250 GB SATA ドライブ	300 GB SAS RAID ドライブ × 2	300 GB SFF SAS RAID ドライブ × 4
リムーバブルメディア	CD/DVD-ROM ドライブ	CD/DVD-ROM ドライブ	CD/DVD-ROM ドライブ
<b>ネットワーク接続</b>			
イーサネット Network Interface Card (NIC; ネットワークインターフェイスカード)	Integrated NIC × 2 Gigabit NIC (PCI-X) × 2	Integrated NIC × 2 Gigabit NIC (PCI-X) × 2	Integrated NIC × 2 Gigabit NIC (PCI-X) × 2
10BASE-T ケーブルのサポート	カテゴリ (Cat) 3, 4, または 5 Unshielded Twisted Pair (UTP)、最大 100 m (328 フィート)	Cat 3, 4, または 5 UTP、最大 100 m (328 フィート)	Cat 3, 4, または 5 UTP、最大 100 m (328 フィート)
10/100/1000BASE-T ケーブルのサポート	Cat 5 UTP、最大 100 m (328 フィート)	Cat 5 UTP、最大 100 m (328 フィート)	Cat 5 UTP、最大 100 m (328 フィート)
Secure Sockets Layer (SSL) アクセラレータカード	なし	Cavium CN1120-NHB-E	Cavium CN1120-NHB-E
<b>インターフェイス</b>			
シリアルポート	1	1	1
USB 2.0 ポート	4 (前面: 2, 背面: 2)	4 (前面: 1, 内蔵: 1, 背面: 2)	4 (前面: 1, 内蔵: 1, 背面: 2)
キーボードポート	1	1	1

	Cisco NAC Appliance 3315	Cisco NAC Appliance 3355	Cisco NAC Appliance 3395
ビデオポート	1	1	1
マウスポート	1	1	1
外部 SCSI ポート	なし	なし	なし
<b>システムユニット</b>			
フォームファクタ	ラックマウント 1 RU	ラックマウント 1 RU	ラックマウント 1 RU
重量	12.7 kg (28 ポンド)、フル構成時	15.87 kg (35 ポンド)、フル構成時	15.87 kg (35 ポンド)、フル構成時
寸法	高さ: 43 mm (1.69 インチ) 幅: 440 mm (17.32 インチ) 奥行: 559 mm (22 インチ)	高さ: 43 mm (1.69 インチ) 幅: 440 mm (17.32 インチ) 奥行: 711 mm (27.99 インチ)	高さ: 43 mm (1.69 インチ) 幅: 440 mm (17.32 インチ) 奥行: 711 mm (27.99 インチ)
電源装置	350 W	デュアル 675 W (冗長)	デュアル 675 W (冗長)
冷却ファン	6 (ホットプラグ非対応の非冗長)	9 (冗長)	9 (冗長)
BTU 定格	2661 BTU/Hr@120	2661 BTU/Hr@120	2661 BTU/Hr@120
<b>適合標準規格</b>			
業界認定資格	FIPS 140-2 レベル 2 Common Criteria EAL2	FIPS 140-2 レベル 2 Common Criteria EAL2	FIPS 140-2 レベル 2 Common Criteria EAL2

### システム要件

オプションの Cisco NAC Agent は、表 4 に示した要件を満たすシステム上で動作します。

表 4 Cisco NAC Agent のシステム要件

機能	最小要件
サポート対象 OS	Windows Vista Business、Windows Vista Ultimate、Windows Vista Enterprise、Windows Vista Home、Windows XP Professional、Windows XP Home、Windows XP Media Center Edition、Windows XP Tablet PC、Windows 2000、Windows 98、Windows SE、Windows ME、Mac OS X NAC 4.7.1 の対応 OS 状況については「 <a href="#">NAC 4.7.1 対応 Windows &amp; MAC OS</a> 」をご参照ください。
ハードドライブの空き容量	ハードドライブの空き容量 10 MB 以上
ハードウェア	ハードウェアに関する最小要件はありません (各種クライアント マシンで稼働)

Cisco NAC では、特定の IP Security (IPSec) VPN および WebVPN クライアントを使用する無線およびリモート アクセス ユーザのシングル サインオンもサポートします。表 5 に、サポートされるコンポーネントを示します。

表 5 シングル サインオンがサポートされる VPN および無線コンポーネント

製品	クライアント
Cisco Wireless LAN Controller	–
Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス	<ul style="list-style-type: none"> <li>• Cisco SSL VPN (トンネル)</li> <li>• Cisco IPsec VPN クライアント</li> </ul>
Cisco WebVPN サービス モジュール (Cisco Catalyst® 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用)	
Cisco VPN 3000 シリーズ コンセントレータ	
Cisco PIX® セキュリティ アプライアンス	

Cisco NAC は、50 のベンダーの 350 以上のアプリケーションについて、ポリシー チェックを行うように事前に設定されています。チェックの対象となるアプリケーションは定期的に追加されます。チェック対象のアプリケーションの最新の一覧については、次の URL をご覧ください (「Cisco NAC Appliance Supported AV/AS Product List」を参

照)。 [http://www.cisco.com/en/US/products/ps6128/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html) [英語]

**注:** すべての製品についてすべてのチェックタイプがサポートされているわけではなく、また、ベンダーによっては Windows 9x をサポートしていません。ユーザは、Cisco NAC のルール エンジンにフル アクセスできるため、事前設定されたチェック以外に、他のサードパーティ製アプリケーション用にカスタム チェックやルールを作成できます。

### サービスおよびサポート

シスコは、お客様がそのネットワーク サービスを最大限に活用できるよう、各種サービス プログラムを用意しています。これらのプログラムは、スタッフ、プロセス、ツール、パートナーを独自に組み合わせたかたちで提供され、お客様から高い評価を受けています。ネットワークへの投資を無駄にすることなく、ネットワーク運用を最適化しネットワーク インテリジェンスの強化や事業拡張を進めていただくために、シスコのサービスを是非お役立てください。シスコ サービスの詳細については、[シスコ テクニカル サポートサービス](#)または[シスコ アドバンスド サービス](#)を参照してください。

保証に関する情報は、<http://www.cisco.com/go/warranty/> [英語] を参照してください。ライセンス情報について

は、[http://www.cisco.com/en/US/docs/security/nac/appliance/support\\_guide/license.html](http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html) [英語] を参照してください。

### 関連情報

Cisco NAC の詳細については、<http://www.cisco.com/jp/go/nac/> を参照するか、最寄りの代理店までお問い合わせください。

©2011 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R) この資料に記載された仕様は予告なく変更する場合があります。



#### 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/>

#### お問い合わせ先