サービス統合型ルータ用 Cisco NAC ネットワーク モジュール

概要

Q. Cisco® Network Admission Control（NAC）とは何ですか。

A. Cisco Network Admission Control（NAC）は、ネットワーク インフラストラクチャを使用して、ネットワーク コンピューティング リソースにアクセスするすべてのデバイスにセキュリティ ポリシーを適用するソリューションです。Cisco NAC により、全社的にすべてのホストが最新のアンチウイルス、セキュリティ ソフトウェア、および OS パッチなどのセキュリティ ポリシーに適合していることを確認したうえで、通常どおりのネットワーク アクセスを許可することができます。脆弱性のある不適合なホストは、適合するまで分離（隔離）されたり、アクセスが制限されたりします。さらに、適切なユーザ クレデンシャルを持つデバイスのみがネットワーク アクセスを許可されるように、Cisco NAC はネットワーク レベルでユーザ認証を実行できます。

Q. サービス統合型ルータ用 Cisco NAC ネットワーク モジュールとは何ですか。

A. サービス統合型ルータ用 Cisco NAC ネットワーク モジュール（NME-NAC-K9）を使用すると、Cisco ISR 2800 および 3800 シリーズで、Cisco NAC Server（NAC Server）の豊富な機能を利用できるようになります。Cisco NAC アプライアンス製品が小さな拠点でも使用でき、本社でもブランチ オフィスでも NAC の機能を利用できるようになります。オンラインの同時ユーザの数に基づいて 2 つのソフトウェア ライセンス（50 ユーザと 100 ユーザ）を選択できる、単一ハードウェア構成のサービス統合型ルータ用ネットワーク モジュールです。

Q. サービス統合型ルータ用 Cisco NAC ネットワーク モジュールの利点は何ですか。

A. NAC Server の機能がサービス統合型ルータ用ネットワーク モジュールに組み込まれているため、データ、音声、およびセキュリティの要件に応じてネットワーク管理者がブランチ オフィスで管理するデバイスが 1 台で済みます。これにより、ネットワーク構成を簡素化し、IT スタッフのトレーニング、必要となる機器の数およびメンテナンス コストの削減が可能になります。また、サービス統合型ルータ用 Cisco NAC ネットワーク モジュールをブランチ オフィスに導入することで、潜在的な脅威が WAN を通過してネットワークに感染する前に、ローカルで修復できます。サービス統合型ルータに Cisco NAC ネットワーク モジュールを搭載したネットワークでは、次の機能を利用できます。

- 適合性をアクセスの条件にすることで機密を保持
- ウイルス、ワーム、スパイウェア、およびその他の悪意のあるアプリケーションに対する予防的な防御
- 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制
- ユーザ マシンの修復および更新プロセスを自動化することでコストを大幅に削減
- 導入における柔軟性と総所有コストの削減

Q. Cisco NAC ネットワーク モジュールは、Cisco NAC アプライアンス製品全体にどのように組み込まれますか。

A. Cisco NAC アプライアンス ソリューションには、次の 3 つのコンポーネントがあります。

- **NAC Server（Clean Access Server）**：NAC Server は、評価を開始して、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アクセス権限を決定するデバイスで、オンラインの同時ユーザの数に基づいて、6 つのサイズ（100、250、500、1500、2500、および 3500 ユーザ）が用意されています。Cisco NAC ネットワーク モジュールの導入により、NAC Server にはオンラインの同時ユーザの数に基づいて、2 つのサイズ（50 ユーザと 100 ユーザ）も用意されています。

  1 社でサイズの異なる複数のサーバを使用できます。たとえば、本社ビルでは Cisco NAC 3350 アプライアンスを使用する 1500 ユーザの NAC Server を使用し、同じ会社のブランチ オフィスでは、Cisco ISR 2800 または 3800 に搭載された Cisco NAC ネットワーク モジュールを使用する 100 ユーザのみのサーバを使用できます。

- **NAC Manager（Clean Access Manager）**：NAC Manager は、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 Web ベースのコンソールで、3 つのサイズが用意されています（アプライアンスのみ）。Lite Manager は最大 3 台の NAC Server、Standard Manager は最大 20 台の NAC Server、Super Manager は最大 40 台の NAC Server を管理します。NAC Manager を使用すると、ネットワーク モジュールとアプライアンスの両方のタイプの NAC Server を設定して管理できます。

- **NAC Agent（Clean Access Agent）**：この読み取り専用のエージェントは、ポスチャ評価機能を強化し、修復作業を効率化します。NAC Agent はオプションであり、無料で配布されます。

製品の詳細

Q. Cisco NAC ネットワーク モジュールには、Cisco NAC アプライアンスと同じ機能がありますか。

A. はい。Cisco NAC アプライアンスの NAC Server の機能はすべて、Cisco NAC ネットワーク モジュール（NME-NAC-K9）でサポートされています（ハイ アベイラビリティを除く）。

Q. Cisco NAC ネットワーク モジュールがサポートできる同時ユーザの数は何人ですか。

A. Cisco NAC ネットワーク モジュールは、最大 100 人の同時ユーザをサポートできます。サポートされるユーザの数は、ネットワーク モジュールと同時に発注するソフトウェア ライセンスによって決まります。最大 50 ユーザの Cisco NAC ネットワーク モジュール サーバ ライセンス（製品番号 NACNM-50-K9）、最大 100 ユーザの Cisco NAC ネットワーク モジュール サーバ ライセンス（製品番号 NACNM-100-K9）があります。

Q. NAC ネットワーク モジュールをサポートする Cisco ルータはどれですか。

A. Cisco NAC ネットワーク モジュールは、ネットワーク モジュール スロットを装備したモジュラ サービス統合型ルータ（Cisco ISR 2811、2821、2851、3825、および 3845 プラットフォーム）でサポートされています。Cisco NAC ネットワーク モジュールは、Cisco 3700 または 2600XM ルータではサポートされていません。

Q. NAC ネットワーク モジュールをサポートするためのホストとなるサービス統合型ルータの Cisco IOS ソフトウェア要件は何ですか。

A. NAC ネットワーク モジュール（NME-NAC-K9）をサポートするためには、Cisco IOS ソフトウェア リリース 12.4(11)T 以上（IP Base イメージ以上）を実行する Cisco サービス統合型ルータ プラットフォームが必要です。

Q. NAC ネットワーク モジュールで実行されるソフトウェアは何ですか。

A. 製品の投入時には、NAC ネットワーク モジュールは NAC Server ソフトウェア バージョン 4.1.2 を実行します。NAC アプライアンス用の新機能が開発された場合、最新バージョンの NAC Server ソフトウェアをインストールすることで、Cisco NAC ネットワーク モジュールに新機能を導入できます。

Q. Cisco ISR 2800 および 3800 に搭載できる NAC ネットワーク モジュールはいくつですか。

A. 1 つです。現在、Cisco ISR 2800 または 3800 に搭載できる NAC ネットワーク モジュールは 1 つのみです。ブランチ オフィスで 100 人を超えるユーザをサポートする必要がある場合は、適切なサイズの NAC Server を利用可能な NAC アプライアンスを導入することを推奨します。

設定および導入

Q. サービス統合型ルータ用 Cisco NAC ネットワーク モジュールは、どのように設定および管理すればよいですか。

A. サービス統合型ルータ用 Cisco NAC ネットワーク モジュールは、主に NAC Manager（ネットワーク全体用に別個のアプライアンスとして導入）の Web ベースの GUI を使って設定および管理できます。NAC ネットワーク モジュールの初期設定は、ルータの CLI（コマンドライン インターフェイス）とモジュールへのリバース Telnet セッションを使用して行われます。これには、NAC ネットワーク モジュールの信頼される（内部）ポートへの IP アドレスの割り当てが含まれます。必要に応じて、NAC ネットワーク モジュールの信頼されるポートの IP アドレスにブラウザでアクセスして、NAC Server のサポート ログを取得できます。

Q. NAC Manager は、両方のタイプの NAC Server（NAC ネットワーク モジュールと NAC アプライアンス）を同時に設定および管理できますか。

A. はい。NAC Manager は、NAC ネットワーク モジュールと NAC アプライアンス サーバの両方を同時に管理できます。NAC Manager には、3 つのサイズが用意されています。Lite Manager は最大 3 台の NAC Server、Standard Manager は最大 20 台の NAC Server、Super Manager は最大 40 台の NAC Server を管理します。NAC Server 数の点では、NAC Manager は NAC ネットワーク モジュールと NAC アプライアンス サーバを同等に扱います。

Q. NAC ネットワーク モジュールは、インバンド モードとアウトオブバンド モードの両方で動作しますか。

A. はい。NAC アプライアンスとしての NAC Server の既存の導入方法はすべて、NAC ネットワーク モジュールでサポートされます。サービス統合型ルータに搭載された NAC ネットワーク モジュールは、エッジでの導入例です（中央集中型の導入モデルは、NAC ネットワーク モジュールには該当しません）。NAC ネットワーク モジュールの導入オプションについては、表 1を参照してください。

表 1 Cisco NAC ネットワーク モジュールの導入オプション

導入モデル	オプション
トラフィック通過モード	• バーチャル ゲートウェイ（ブリッジド モード） • リアル IP ゲートウェイ（ルーテッド モード）
クライアント アクセス モード	• レイヤ 2（クライアントは NAC Server に隣接） • レイヤ 3（クライアントは NAC Server から複数ホップ先）
トラフィック フロー モデル	• インバンド（NAC Server は常にユーザ トラフィックに対してインラインで動作） • アウトオブバンド（NAC Server は認証、ポスチャ評価、および修復時のみインライン）

Q. NAC ネットワーク モジュールのハードウェア仕様はどのようになっていますか。

A. NAC ネットワーク モジュールは、サービス統合型ルータ用の Linux ベース サービス エンジンで、NAC Server アプリケーションを実行します。ハードウェア アーキテクチャは、1 GHz プロセッサ、512 MB Double-Data-Rate 2（DDR2）RAM、80 GB Serial ATA（SATA）ハード ディスク、64 MB コンパクト フラッシュ モジュールに基づいています。また、ルータ バックプレーンへの内部 1000 Mbps イーサネット インターフェイス× 1 と、外部 10/100/1000 Mbps イーサ

ネット インターフェイス × 1 の 2 つのイーサネット Network Interface Card（NIC; ネットワーク インターフェイス カード）を装備しています。詳細については、データ シートを参照してください。

Q. NAC ネットワーク モジュールの信頼できるインターフェイスと信頼できないインターフェイスはどれですか。

A. 外部から確認できる NAC ネットワーク モジュールのインターフェイスは信頼できないインターフェイスで、ブランチ オフィス内のローカル LAN ネットワークのトラフィックがこのインターフェイスを介してネットワーク モジュールとルータに着信します。NAC ネットワーク モジュール上の信頼できるインターフェイスは、モジュールの内部にあり、ギガビット イーサネット ポートを介してホスト サービス統合型ルータのバックプレーンに接続されます。

Q. ルータ CLI から NAC ネットワーク モジュールへの「リバース Telnet」接続は、どのように動作しますか。

A. リバース Telnet は、ルータからモジュールへの内部仮想 Telnet インターフェイスを使用します。service-module g x/y session コマンドを使用して、実際の CLI にアクセスできます。この方法により、外部コンソール接続を使用しなくても、モジュールへのコンソール タイプのアクセスが許可されます。

Q. NAC ネットワーク モジュールとホスト ルータ上のソフトウェア イメージを個別にアップグレードできますか。

A. はい。Cisco IOS ソフトウェア リリースの最小要件を満たしているかぎり、ルータまたは NAC ネットワーク モジュール上のイメージを変更できます。NAC ネットワーク モジュール アプリケーション イメージを個別にアップグレードし、ルータに影響を与えることなくモジュールをリブートおよびリロードできます。

Q. ソフトウェア イメージは、NAC ネットワーク モジュールにどのようにロードされるのですか。

A. TFTP サーバを使用して、NAC Server アプリケーション イメージを NAC ネットワーク モジュールにロードできます。詳細については、製品マニュアルを参照してください。

サービス統合型ルータの統合と相互運用性

Q. Cisco NAC ネットワーク モジュールは、Cisco High-Speed Intrachassis Module Interconnect（HIMI）機能をサポートしていますか。

A. はい。ネットワーク モジュールは Cisco HIMI 機能をサポートしています。Cisco HIMI 機能により、Enhanced Network Module（NME）と、別の NME、または Cisco ISR 3825 または 3845 のオンボード ギガビット イーサネット Small Form-Factor Pluggable（SFP）ポートとの間に専用のポイントツーポイント内部接続を確立できます。HIMI 機能は、最大 1 Gbps まで拡張できるレイヤ 2 接続で、ルータ シャーシごとに最大 2 台の NME をサポートします。現在のところ、HIMI をサポートする NME には Cisco EtherSwitch® サービス モジュールがあります。この機能を使用すると、Cisco NAC ネットワーク モジュールと、Cisco EtherSwitch サービス モジュールなどの他の HIMI 対応拡張ネットワーク モジュールの間で、高度な統合を実現できます。HIMI の詳細については、http://www.cisco.com/en/US/products/ps5855/prod_configuration_guide09186a008068ea83.html#wp1047623 を参照してください。

Q. Cisco NAC ネットワーク モジュールは、同じサービス統合型ルータ内に Cisco EtherSwitch サービス モジュールと共に導入できますか。

A. はい。NAC ネットワーク モジュール（NME-NAC-K9）は、同じシャーシ内で Cisco EtherSwitch サービス モジュール（製品番号 NME-16ES-1G-P、NME-X-23ES-1G-P、

NME-XD-24ES-1S-P、NME-XD-48ES-2S-P、NME-16ES-1G、または NME-X-23ES-1G）と相互運用できます。Cisco EtherSwitch モジュールに接続された端末（ノート型パソコン、PC、IP フォンなど）からのローカル LAN トラフィックを、NAC ネットワーク モジュールの信頼されていないポートに転送し、ルータから WAN へ送信される前に NAC ネットワーク モジュールでユーザ トラフィックを評価できます。Cisco ISR 3825 または 3845 では、この 2 つの拡張モジュール（Cisco NAC ネットワーク モジュールおよび Cisco EtherSwitch サービス モジュール）を、内蔵の高速リンク（HIMI）を使用して直接接続できます。

Q. Cisco NAC ネットワーク モジュールは、同じサービス統合型ルータ内に Cisco Wireless LAN Controller モジュールと共に導入できますか。

A. はい。NAC ネットワーク モジュールは、同じシャーシ内で Cisco Wireless LAN Controller モジュール（製品番号 NM-AIR-WLC6-K9、NME-AIR-WLC8-K9、または NME-AIR-WLC12-K9）と相互運用できます。この環境では、ワイヤレス（および有線）LAN トラフィックを、サービス統合型ルータのオンボード ギガビット イーサネット インターフェイスから、NAC ネットワーク モジュールの信頼されていないインターフェイスにポリシー ルーティングする必要があります。これにより、一部のトラフィックがルータを 2 回通過するため、パフォーマンスに影響する可能性があります。

予測されるホスト ルータのサービス負荷が大きい場合、アプライアンス（Cisco 2100 または 4400 シリーズ Wireless LAN Controller）として、またはスイッチ（Cisco Catalyst® 3750 シリーズ）として、NAC ネットワーク モジュールと共にワイヤレス LAN コントローラを導入できます。また、NAC Server を、サービス統合型ルータ内のネットワーク モジュールとしてではなく、アプライアンス（Cisco NAC 3300 アプライアンス）としてワイヤレス LAN コントローラ（NME-AIR-WLC）と共に導入することもできます。

Q. Cisco NAC ネットワーク モジュールは、ワイヤレス ユーザのシングル サインオン（SSO）をサポートしていますか。

A. はい。ルータは、RADIUS アカウンティング サーバとして NAC ネットワーク モジュールを使用するように設定する必要があります。ユーザがワイヤレス ネットワークにログインすると、RADIUS アカウンティング メッセージを通じてログイン クレデンシャルが NAC ネットワーク モジュールに提供されます。ログイン クレデンシャルが有効な場合、NAC ネットワーク モジュールは、2 回めにネットワークにアクセスする際、ユーザに対してログインを要求しません。.

Q. Cisco NAC ネットワーク モジュールは、ホスト ルータで設定された Cisco IOS Firewall およびサイト間 VPN と共に導入できますか。

A. はい。ルータで設定された Cisco IOS Firewall およびサイト間 VPN と共に導入できます。

Q. Cisco NAC ネットワーク モジュールは、リモート アクセス VPN（IPSec および SSL VPN）を終端するように設定されたサービス統合型ルータに導入できますか。

A. はい。NAC ネットワーク モジュールは、リモート アクセス VPN 接続を終端するサービス統合型ルータと相互運用するように設定できます。この環境では、リモート アクセス VPN ユーザからの復号化されたトラフィックを、サービス統合型ルータのオンボード ギガビット イーサネット インターフェイスから、NAC ネットワーク モジュールの信頼されていないインターフェイスにポリシー ルーティングする必要がありますが、一部のトラフィックがルータを 2 回通過するため、パフォーマンスに影響する可能性があります。

Q. Cisco NAC ネットワーク モジュールは、リモート アクセス VPN ユーザ（IPSec および SSL VPN）の SSO をサポートしていますか。

A. はい。IPSec の場合、ルータは、RADIUS アカウンティング サーバとして NAC ネットワーク モジュールを使用するように設定されます。ユーザが VPN ネットワークにログインすると、RADIUS アカウンティング メッセージを通じてログイン クレデンシャルが NAC ネットワーク モジュールに提供されます。ログイン クレデンシャルが有効な場合、NAC ネットワーク モジュールは、2 回めにネットワークにアクセスする際、ユーザに対してログインを要求しません。SSL VPN での SSO のサポートは、Cisco NAC アプライアンス リリース 4.1.3 以降で利用できるようになります。

発注、ライセンスなど

Q. サービス統合型ルータ用 Cisco NAC ネットワーク モジュールの発注方法を教えてください。

A. Cisco ISR 2800 または 3800 シャーシまたはバンドルを構成する場合は、ネットワーク モジュールのオプションとして NAC ネットワーク モジュールを選択してください。NAC ネットワーク モジュールのソフトウェア バージョンを確認したあと、2 つの Cisco NAC ネットワーク モジュール サーバ ライセンス（製品番号 NACNM-50-K9 または NACNM-100-K9）のいずれかを選択してください。NAC ネットワーク モジュールの 50 ユーザ ライセンス（NACNM-50-K9）を最初に購入した場合は、製品番号 NACNM-50UL= を発注することで 100 ユーザ ライセンスにアップグレードできます。モジュールのスペア（NME-NAC-K9=）に対しても、同様にすべてのライセンスを選択して適用できます。詳細については、表 2 を参照してください。

表 2 サービス統合型ルータ用 Cisco NAC ネットワーク モジュールの発注情報

ハードウェアとソフトウェアの製品番号	Cisco NAC ネットワーク モジュールのサポートに必要なもの
NME-NAC-K9	ISR 2800/3800 用 Cisco NAC ネットワーク モジュール
NACNM-50-K9	NAC ネットワーク モジュール サーバ ライセンス（最大 50 ユーザ）
NACNM-100-K9	NAC ネットワーク モジュール サーバ ライセンス（最大 100 ユーザ）
NACNM-50UL=	NAC ネットワーク モジュール サーバ ライセンス アップグレード（50 から 100 ユーザ）
NME-NAC-K9=	ISR 2800/3800 用 Cisco NAC ネットワーク モジュール（スペア）

Q. NAC ネットワーク モジュールのユーザ ライセンスはアップグレードできますか。

A. はい。NAC ネットワーク モジュールは、製品番号 NACNM-50UL= を発注することで、最初の 50 ユーザ ライセンスから 100 ユーザ ライセンスにアップグレードできます。ライセンスの詳細については、http://www.cisco.com/en/US/products/ps6128/prod_pre_installation_guide09186a008073136b.html を参照してください。

Q. スペアの Cisco NAC ネットワーク モジュールを購入することはできますか。

A. はい。ネットワーク内にサービス統合型ルータをすでに導入している場合、Cisco NAC ネットワーク モジュールをスペア（発注製品番号 NME-NAC-K9=）として発注できます。スペアの拡張ネットワーク モジュールを発注する場合も、ソフトウェアとライセンスには同じ製品番号を使用できます。

Q. Cisco NAC ネットワーク モジュールから Cisco NAC アプライアンスへライセンスをアップグレードすることはできますか。

A. いいえ。NAC ネットワーク モジュールと NAC アプライアンスは、基本的には異なるハードウェア プラットフォームのため、一方から他方へライセンスをアップグレードすることはできません。

特定の場所のユーザ数が 100 ユーザを超えると予測される場合、シスコでは、NAC Server を NAC アプライアンスとして導入することを推奨します。

Q. NAC ネットワーク モジュールには個別のテクニカル サービス（サポート）契約が必要ですか。

A. いいえ。ホスト ルータ用（Cisco ISR 2800 または 3800）のテクニカル サービス契約を購入した場合、NAC ネットワーク モジュールのサポートが含まれています。ただし、ネットワークの中央に（NAC アプライアンスとして）導入される NAC Manager の個別のサービス契約を購入する必要があることに注意してください。

関連情報

Cisco NAC アプライアンスの詳細については、http://www.cisco.com/jp/go/isr および http://www.cisco.com/jp/go/nac/appliance を参照してください。

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）
http://www.cisco.com/jp/go/contactcenter
0120-092-255（通話料無料）
電話受付時間：平日10:00～12:00、13:00～17:00

お問い合せ先

07.11