CISCO SYSTEMS

ネットワーク アドミッション コントロール ドキュメンテーション リファレンス ガイド

2006 年 1 月 31 日

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

OL-87501-01

ネットワーク アドミッション コントロール（NAC）ドキュメンテーション リファレンス ガイド

NAC フレームワークに関するドキュメンテーション 2

NAC フレームワークに関する Web リソース 3

NAD に関するドキュメンテーション 3

Cisco スイッチに関するドキュメンテーション 3

Cisco ルータに関するドキュメンテーション 8

Cisco IOS および CatOS リファレンス ツール 11

Cisco Feature Navigator 11

Command Lookup Tool 11

Cisco Aironet ワイヤレス アクセス ポイントに関するドキュメンテーション 11

Cisco Wirelss LAN Controller 12

Cisco VPN コンセントレータ に関するドキュメンテーション 13

Cisco Secure Access Control Server（ACS）に関するドキュメンテーション 15

Cisco Secure ACS for Windows（V.4.0） 15

Cisco Trust Agent（CTA）に関するドキュメンテーション 15

追加された NAC 対応コンポーネント 16

CSA に関するドキュメンテーション 16

Cisco Secure Monitoring Analysis and Response Systems（CS-MARS） 17

ネットワーク アドミッション コントロール（NAC） ドキュメンテーション リファレンス ガイド

Network Admission Control（NAC; ネットワーク アドミッション コントロール）リリース 2.0（NAC 2.0）は、さまざまなシスコ コンポーネントで構成されるネットワーク セキュリティ ソリューションです。NAC は、ネットワーク インフラストラクチャを活用して、ネットワーク コンピューティング リソースにアクセスしようとするデバイスにセキュリティ ポリシーへの適合を強制することにより、セキュリティの脅威がもたらす損害を抑制します。

NAC を利用することによって、ポリシーに適合する信頼できるエンドポイント デバイス（PC、サーバ、PDA など）にはネットワーク アクセスを許可し、ポリシーに非適合のデバイスに対してはアクセスを制限できます。

基本的な NAC 環境は、Network Access Device（NAD; ネットワーク アクセス デバイス）、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サーバ、NAC 対応ホスト上で稼動するポスチャ エージェントの 3 つのコンポーネントで構成されます。通常、NAD は Cisco ルータまたはスイッチ、AAA サーバは Cisco Secure Access Control Server（ACS）、ポスチャ エージェントは Cisco Trust Agent（CTA）です。拡張された NAC 環境では、ホスト上で追加された NAC 対応アプリケーションが稼動しています。

このドキュメントでは、シスコシステムズの Web サイトで入手できる NAC に関するドキュメンテーション名とそのロケーションをご紹介します。

本書は次のセクションで構成されています。

- NAC フレームワークに関するドキュメンテーション　2 ページ
- NAC フレームワークに関する Web リソース　3 ページ
- NAD に関するドキュメンテーション　3 ページ
  - Cisco スイッチに関するドキュメンテーション　3 ページ
  - Cisco ルータに関するドキュメンテーション　8 ページ
  - Cisco IOS および CatOS リファレンス ツール　11 ページ
  - Cisco Aironet ワイヤレス アクセス ポイントに関するドキュメンテーション　11 ページ
  - Cisco VPN コンセントレータ に関するドキュメンテーション　13 ページ
- Cisco Secure Access Control Server（ACS）に関するドキュメンテーション　15 ページ
  - Cisco Secure ACS for Windows（V.4.0）　15 ページ
- Cisco Trust Agent（CTA）に関するドキュメンテーション　15 ページ
- 追加された NAC 対応コンポーネント　16 ページ
  - CSA に関するドキュメンテーション　16 ページ
  - Cisco Secure Monitoring Analysis and Response Systems（CS-MARS）　17 ページ

NAC フレームワークに関するドキュメンテーション

NAC ソリューションに関する包括的な説明は、以下のドキュメントに記載されています。

- Network Admission Control 2.0 リリース ノート
- Network Admission Control Software コンフィギュレーション ガイド
- ネットワーク アドミッション コントロールの実装
- Network Admission Control Framework コンフィギュレーション ガイド
- ネットワーク アドミッション コントロール Q&A

NAC フレームワークに関する Web リソース

NAC ソリューションについては、以下の Web サイトも参照してください。

- ネットワーク アドミッション コントロール Web サイト
- Network Admission Control（NAC）パートナー
- Network Admission Control 概要（デモンストレーション）
- ネットワーク アドミッション コントロール 技術資料

NAD に関するドキュメンテーション

ネットワーク アクセス デバイス（NAD）は、自身がアクセスを仲介するネットワーク内のリソースにどのホストがアクセスできるかを制御します。特定のホストに適用するアクセス制御は、Cisco Secure ACS が NAD に提供するネットワーク アクセス ポリシーによって定義されます。

Cisco スイッチに関するドキュメンテーション

ホストは、IEEE 802.1X プロトコルまたは Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）を使用してポスチャ情報とアイデンティティ情報をスイッチに提供します。スイッチは、この情報を Cisco Secure ACS に渡します。ACS は、受信したポスチャ情報とアイデンティティ情報に基づいてこのホストのセキュリティ ポリシーを発行し、スイッチにこのポリシーを返します。ホストのセキュリティ ポリシーは、OSI（Open System Interconnection）参照モデルのレイヤ 2 でスイッチによって適用されます。

レイヤ 2 で IEEE 802.1X プロトコルを使用して NAC を実施する場合は、NAC L2 802.1X 方式が使用されます。レイヤ 2 で EAPoUDP プロトコルを使用して NAC を実施する場合には、NAC L2 IP 方式が使用されます。

表 1 に NAC 対応スイッチとこれらのスイッチがサポートする NAC 方式を示します。

表 1　スイッチに関するドキュメンテーション

サポートするプラットフォームとモデル	サポートするNAC 方式	オペレーティングシステム イメージ	関連ドキュメント
Cisco Catalyst 2940	NAC L2 802.1X	Cisco IOS Release 12.1（22）EA6 またはそれ以降	Cisco Catalyst 2940 シリーズ スイッチ 製品ページ Catalyst 2955、Catalyst 2950、Catalyst 2940 スイッチ Cisco IOS Release 12.1（22）EA6 リリース ノート Network Admission Control ソフトウェア コンフィギュレーション ガイド Cisco IOS ソフトウェアのドキュメンテーション
Catalyst 2950 Catalyst 2955	NAC L2 802.1X	Cisco IOS Release 12.1（22）EA6 またはそれ以降	Cisco Catalyst 2950 シリーズ スイッチ 製品ページ Cisco Catalyst 2955 シリーズ スイッチ 製品ページ Catalyst 2955、Catalyst 2950、Catalyst 2940 スイッチ Cisco IOS Release 12.1（22）EA6 リリース ノート Network Admission Control ソフトウェア コンフィギュレーション ガイド Cisco IOS ソフトウェアのドキュメンテーション
Cisco Catalyst 2960	NAC L2 802.1X	Cisco IOS Release 12.2（25）SED またはそれ以降	Cisco Catalyst 2960 シリーズ スイッチ のドキュメンテーション Catalyst 3750、3560、2970、2960 スイッチ Cisco IOS Release 12.2（25）SED リリースノート Network Admission Control ソフトウェア コンフィギュレーション ガイド Cisco IOS ソフトウェアのドキュメンテーション

表 1　スイッチに関するドキュメンテーション（続き）

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
Cisco Catalyst 2970	NAC L2 802.1X	Cisco IOS Release 12.2（25）SED またはそれ以降	Cisco Catalyst 2970 シリーズ スイッチ 製品ページ Catalyst 2970 スイッチ コマンド リファレンス Cisco IOS Release 12.2（25）SED Catalyst 2970 スイッチ ソフトウェア コンフィギュレーション ガイド Cisco IOS Release 12.2（25）SED Catalyst 3750、3560、2970、2960 スイッチ Cisco IOS Release 12.2（25）SED リリース ノート Network Admission Control ソフトウェア コンフィギュレーション ガイド Cisco IOS ソフトウェアのドキュメンテーション
Cisco Catalyst 3550	NAC L2 IP NAC L2 802.1X	Cisco IOS Release 12.2（25）SED またはそれ以降	Catalyst 3550 マルチレイヤ スイッチ Cisco IOS Release 12.2(25) SED リリース ノート Cisco IOS ソフトウェアのドキュメンテーション
Cisco Catalyst 3550	NAC L2 802.1X	Cisco IOS Release 12.1（22）EA6 またはそれ以降	Cisco Catalyst 3550 シリーズ スイッチ 製品ページ Network Admission Control ソフトウェア コンフィギュレーション ガイド Cisco IOS ソフトウェアのドキュメンテーション

表 1　スイッチに関するドキュメンテーション（続き）

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
Cisco Catalyst 3560	NAC L2 IP NAC L2 802.1X	Cisco IOS Release 12.2（25）SED またはそれ以降	Cisco Catalyst 3560 シリーズ スイッチ 製品ページ Catalyst 3560 スイッチ コマンド リファレンス Cisco IOS Release 12.2（25）SED Catalyst 3560 スイッチ ソフトウェア コンフィギュレーション　ガイド Cisco IOS Release 12.2（25）SED Catalyst 3750、3560、2970、2960 スイッチ Cisco IOS Release 12.2（25）SED リリース ノート Network Admission Control ソフトウェア コンフィギュレーション ガイド Cisco IOS ソフトウェアのドキュメンテーション
Cisco Catalyst 3750	NAC L2 IP NAC L2 802.1X	Cisco IOS Release 12.2（25）SED またはそれ以降	Cisco Catalyst 3750 シリーズ スイッチ 製品ページ Catalyst 3750 スイッチ コマンド リファレンス Cisco IOS Release 12.2（25）SED Catalyst 3750 スイッチ ソフトウェア コンフィギュレーション ガイド Cisco IOS Release 12.2（25）SED Catalyst 3750、3560、2970、2960 スイッチ Cisco IOS Release 12.2（25）SED リリース ノート Network Admission Control ソフトウェア コンフィギュレーション ガイド Cisco IOS ソフトウェアのドキュメンテーション

表 1　スイッチに関するドキュメンテーション（続き）

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
Cisco Catalyst 4500 Cisco Catalyst 4900	NAC L2 IP NAC L2 802.1X	Cisco IOS 12.2（25）SG またはそれ以降	Catalyst 4500 スイッチ 製品ページ Catalyst 4900 スイッチ 製品ページ Catalyst 4500 スイッチ ドキュメンテーション ロードマップ Catalyst 4500 シリーズ スイッチ Cisco IOS コマンド リファレンス 12.2（25）SG Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド 12.2（25）SG Network Admission Control ソフトウェア コンフィギュレーション ガイド Cisco IOS ソフトウェアのドキュメンテーション
Cisco 6500 シリーズ モデル： 6503、6503-E、6506、6506-E、6509、6509-E、6509-NEB、6509-NEB-A、6513	NAC L2 IP	Cisco IOS 12.2（18）SXF2	Catalyst 6500 シリーズ Cisco IOS ソフトウェア ドキュメンテーション 12.2SX Supervisor Engine 720、Supervisor Engine 32、Supervisor Engine 2 Cisco IOS Release 12.2SX リリース ノート Cisco IOS ソフトウェアのドキュメンテーション

表 1　スイッチに関するドキュメンテーション（続き）

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
Cisco 6500 シリーズ モデル： 6503、6503-E、6506、6506-E、6509、6509-E、6509-NEB、6509-NEB-A、6513	NAC L2 IP NAC L2 802.1X	CatOS 8.5 またはそれ以降	Catalyst 6500 スイッチ 製品ページ Catalyst 6500 ドキュメンテーション ロードマップ 8.5 Catalyst 6500 シリーズ コマンド リファレンス 8.5 Catalyst 6500 シリーズ ソフトウェア コンフィギュレーション ガイド 8.5 Network Admission Control ソフトウェア コンフィギュレーション ガイド

Cisco ルータに関するドキュメンテーション

ホストは、Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）を使用してポスチャ情報をルータに提供し、ルータはこの情報を ACS に渡します。ACS は、受信したポスチャ情報に基づいてこのホストのセキュリティ ポリシーを発行し、ルータにこのポリシーを返します。このホストのセキュリティ ポリシーは、OSI 参照モデルの レイヤ 3 でルータによって適用されます。EAPoUDP 方式を使用してレイヤ 3 で NAC を実施する手法は、NAC L3 IP 方式と呼ばれます。

表 2 に NAC 対応ルータとこれらのルータがサポートする NAC 方式を示します。

表 2　ルータに関連するドキュメンテーション

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
Cisco 830 および 870 シリーズ モデル：831、836、837	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco 800 シリーズ ルータ 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション

表 2　ルータに関連するドキュメンテーション（続き）

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
Cisco 1700 シリーズ モデル：1701、1711、1712、1721、1751、1751-V、1760	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco 1700 シリーズ モジュラ アクセス ルータ 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション
Cisco ISR 1812J	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	
Cisco ISR 1800 シリーズ モデル：1841	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco ISR 1800 シリーズ サービス統合型ルータ 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション
Cisco 2600 シリーズ モデル：2600XM、2691	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco 2600 シリーズ マルチサービス プラットフォーム 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション
Cisco ISR 2800 シリーズ モデル：2801、2811、2821、2851	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco ISR 2800 シリーズ サービス統合型ルータ 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション
Cisco 3600 シリーズ モデル：3640/3640A、3660-ENT シリーズ	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco 3600 シリーズ マルチサービス プラットフォームのドキュメンテーション Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション

表 2　ルータに関連するドキュメンテーション（続き）

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
Cisco 3700 シリーズ モデル：3725、3745	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco 3700 シリーズ マルチサービス アクセス ルータのドキュメンテーション Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション
Cisco 3800 シリーズ モデル：3845、3825	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco ISR 3800 シリーズ サービス統合型ルータ 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション
Cisco 7200 シリーズ	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco 7200 シリーズ ルータ 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション
Cisco 7500 シリーズ	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco 7500 シリーズ ルータ 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション
Cisco 7600 シリーズ	NAC L3 IP	Cisco IOS 12.3（8）T またはそれ以降	Cisco 7600 シリーズ ルータ 製品ページ Cisco IOS Software Releases 12.3 T Cisco IOS ソフトウェアのドキュメンテーション

Cisco IOS および CatOS リファレンス ツール

Cisco Feature Navigator

Cisco Feature Navigator は、お客様が NAD の実装に必要な機能を持つ適切な Cisco IOS および Catalyst OS（CatOS）ソフトウェア リリースを検索できる Web ベース アプリケーションです。このツールは、オンライン ヘルプ、および操作に関する質問とその回答を記載した FAQ を提供します。

Cisco Feature Navigator を使用するには、Cisco.com へのユーザ登録が必要です。

Command Lookup Tool

Command Lookup Tool には、Cisco IOS および Catalyst OS コマンドの構文、デフォルト値、履歴、使用方法、使用例の詳しい説明が含まれています。このツールを使用すると、ご使用のシスコ ルータまたはスイッチのオペレーティング システムの管理に使用されるコマンドの知識を習得できます。

Command Lookup Tool を使用するには、Cisco.com へのユーザ登録が必要です。

Cisco Aironet ワイヤレス アクセス ポイントに関するドキュメンテーション

Cisco Aironet ワイヤレス アクセス ポイントを使用すると、NAC 環境で無線エンドポイントをサポートできます。また、無線エンドポイントをサポートするには、サードパーティ製の IEEE 802.1X サプリカントも必要となります。

『Cisco Aironet アクセス ポイント Cisco IOS ソフトウェア コンフィギュレーション ガイド Cisco IOS Release 12.3（7）JA』には、NAC 環境における Aironet Wireless Access Point についての説明が記載されています。

表 3　Cisco Aironet ワイヤレス アクセス ポイントに関するドキュメンテーション

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
350 シリーズ	NAC L2 802.1X	IOS releases 12.3（7）JA1 およびそれ以降	Cisco Aironet 350 シリーズ 製品ページ
1100 シリーズ	NAC L2 802.1X	IOS releases 12.3（7）JA1 およびそれ以降	Cisco Aironet 1100 シリーズ 製品ページ

表 3　Cisco Aironet ワイヤレス アクセス ポイントに関するドキュメンテーション（続き）

サポートする プラットフォームとモデル	サポートする NAC 方式	オペレーティング システム イメージ	関連ドキュメント
1130 AG シリーズ	NAC L2 802.1X	IOS releases 12.3（7）JA1 およびそれ以降	Cisco Aironet 1130 AG シリーズ 製品ページ
1200 シリーズ	NAC L2 802.1X	IOS releases 12.3（7）JA1 およびそれ以降	Cisco Aironet 1200 シリーズ 製品ページ
1230 AG シリーズ	NAC L2 802.1X	IOS releases 12.3（7）JA1 およびそれ以降	Cisco Aironet 1230 シリーズ 製品ページ
1240 AG シリーズ	NAC L2 802.1X	IOS releases 12.3（7）JA1 およびそれ以降	Cisco Aironet 1240 AG シリーズ 製品ページ

Cisco Wirelss LAN Controller

Cisco Wirelss LAN Controller は、セキュリティ ポリシー、侵入防止、RF 管理、QoS（Quality of Service）、およびモビリティなどの無線 LAN 機能をシステム全体に提供します。このデバイスは、Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントおよび Cisco Wireless Control System（WCS）と連携して、無線アプリケーションをサポートします。

Cisco Wireless LAN Controller は、Lightweight Access Point Protocol（LWAPP）を使用し、レイヤ 2（イーサネット）またはレイヤ 3（IP）インフラストラクチャで Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントと通信します。また、企業内のすべてのロケーションにおける WLAN に関するさまざまな設定および管理の自動化もサポートしています。

表 4　Wireless LAN Controller に関するドキュメンテーション

サポートする プラットフォームとモデル	サポートする NAC 方式	Cisco Unified Wireless Network ソフトウェア	関連ドキュメンテーション
Cisco 2000	NAC L2 802.1X	Release 3.1 またはそれ以降	Cisco 2000 シリーズ Wireless LAN Controller 製品ページ
Cisco 4100	NAC L2 802.1X	Release 3.1 またはそれ以降	Cisco 4100 シリーズ Wireless LAN Controller 製品ページ
Cisco 4400	NAC L2 802.1X	Release 3.1 またはそれ以降	Cisco 4400 シリーズ Wireless LAN Controller 製品ページ

表 4　Wireless LAN Controller に関するドキュメンテーション（続き）

サポートする プラットフォームとモデル	サポートする NAC 方式	Cisco Unified Wireless Network ソフトウェア	関連ドキュメンテーション
Wireless Services Module（WiSM）	NAC L2 802.1X	Release 3.1 またはそれ以降	Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM）製品ページ
Wireless LAN Services Module（WLSM）	NAC L2 802.1X	Release 3.1 またはそれ以降	Cisco Catalyst 6500 シリーズ Wireless LAN Services Module（WLSM）製品ページ
Cisco ISR 用 Wireless LAN Controller Module	NAC L2 802.1X	Release 3.1 またはそれ以降	Cisco Wireless LAN Controller Module 製品ページ

Cisco VPN コンセントレータ に関するドキュメンテーション

Virtual Private Network（VPN）コンセントレータは、NAC オーセンティケータおよび ACS クライアントの両方として機能します。VPN コンセントレータはレイヤ 3 デバイスと考えられており、ポスチャ認証に NAC L3 IP 方式を使用します。

VPN コンセントレータは、NAC オーセンティケータとして、次のタスクを実行します。

- 確立された IPSec セッションをベースに最初のクレデンシャル交換を開始する。その後も定期的に交換を開始する。
- Protected Extensible Authentication Protocol（PEAP）を使用してピアと認証（ACS）サーバ間のクレデンシャル要求および応答を中継する
- ACS サーバから返された結果に基づいて IPSec セッションにネットワーク アクセス ポリシーを適用する
- 設定された EAP Status Query 方式を実行する
- ピアのオペレーティング システムに基づいたローカル例外リストをサポートする
- クライアントレス ホストに適用するアクセス ポリシーを ACS サーバに要求する

また VPN コンセントレータは、ACS クライアントとして次の要素をサポートしています。

- EAP/RADIUS
- NAC に必要な RADIUS 属性

VPN 3000 コンセントレータにおける NAC は、ルータなどの Cisco IOS レイヤ 3 デバイスにおける NAC とは異なります。ルータの場合、ポスチャ認証（PV）はルーティングされたトラフィックによって開始されますが、NAC が設定された VPN 3000 コンセントレータの場合、PV は IPSec VPN セッションの確立によって開始されます。NAC が設定された Cisco IOS ルータでは、特定のネットワーク宛てのトラフィックをベースに PV が開始されるため、Intercept ACL（Access Control List）を使用します。外部のデバイスは VPN セッションを開始しなければ VPN 3000 コンセントレータ内部のネットワークにアクセスできないため、VPN コンセントレータは PV の開始時に Intercept ACL を使用する必要はありません。ポスチャ認証中、デバイスからのすべての IPSec トラフィックには、そのデバイスのグループに対して設定されているデフォルト ACL が適用されます。

表 5　VPN コンセントレータに関するドキュメンテーション

サポートする プラットフォームとモデル	オペレーティング システム バージョン	関連ドキュメント
Cisco VPN 3000 シリーズ モデル：3005 ～ 3080	V4.7 またはそれ以降	VPN 3000 ネットワーク アクセス デバイス 4.7.0 NAC アドミニストレーションおよびコンフィギュレーション VPN 3000 ネットワーク アクセス デバイス 4.7.1 NAC アドミニストレーションおよびコンフィギュレーション Cisco VPN 3000 シリーズ コンセントレータ Release 4.7; Cisco SSL VPN クライアント Release 1.0 リリース ノート Cisco VPN 3000 シリーズ コンセントレータ Release 4.7.1 リリース ノート Cisco VPN 3000 シリーズ コンセントレータ Release 4.7.2 リリース ノート

Cisco Secure Access Control Server（ACS）に関するドキュメンテーション

Cisco Secure Access Control Server（ACS）は、NAC の中心となる AAA（認証、許可、アカウンティング）サーバです。

ホストがネットワークへのアクセスを試みると、Cisco Secure ACS はホストのポスチャ クレデンシャルを要求します。Cisco Trust Agent は、ポスチャ プラグインからクレデンシャルを収集して Cisco Secure ACS に渡します。Cisco Secure ACS は、受信したクレデンシャルに基づいてホストの各アプリケーションのポスチャとホストの総合的なポスチャ トークンを決定します。

Cisco Secure ACS は、ホストの総合的なポスチャ トークンをベースにこのホストに適用するネットワーク アクセス ポリシーを定義し、ホストにポリシーを適用する NAD にこのポリシーを転送します。

Cisco Secure ACS for Windows（V.4.0）

Cisco Secure ACS for Windows は、ACS のソフトウェア製品です。

- Cisco Secure ACS for Windows 製品ページ
- Cisco Secure ACS for Windows V.4.0 リリース ノート
- Cisco Secure ACS インストレーション ユーザ ガイド（パスワード変更に対応）
- Cisco Secure ACS for Windows 4.0 インストレーション ガイド
- Cisco Secure ACS for Windows 4.0 ユーザ ガイド
- Cisco Secure ACS for Windows 4.0 サポートおよび相互運用可能なデバイス

Cisco Trust Agent（CTA）に関するドキュメンテーション

Cisco Trust Agent（CTA）は NAC のポスチャ エージェントです。CTA ソフトウェアは、ネットワーク上の各ホストにインストールされます。ホストがネットワークへのアクセスを試みると、ACS はホストのポスチャ クレデンシャルを要求します。CTA は、ポスチャ プラグインからクレデンシャルを収集して Cisco Secure ACS に渡します。各ポスチャ プラグインは、単一のアプリケーションからポスチャ情報を収集します。

Windows ベースのネットワーク クライアントの場合、CTA は Cisco Trust Agent 802.1X Wired Client（802.1X Wired Client）と呼ばれる「サプリカント」とともにインストールできます。802.1X Wired Client は、イーサネット スイッチへのセキュアなユーザ接続を確立するための認証サプリカントです。802.1X Wired Client は、認証ステータスの監視と許可されたネットワーク アクセスの管理に使用できる GUI を提供します。

ネットワークが次のすべての状況に適合する場合には、802.1X Wired Client とともに CTA をインストールします。

- スイッチでホストを認証する
- NAC L2 802.1X（EAP-Flexible Authentication using Secure Tunneling; EAP-FAST Protocol）を使用してスイッチにトラフィックを送信する
- ホストが Windows ベースのオペレーティング システムを実行している

ネットワークが次のいずれかの状況に適合する場合には、802.1X Wired Client のインストールを伴わずに CTA をインストールします。

- スイッチでホストを認証し、NAC L2 IP（EAP over UDP）を使用してスイッチにトラフィックを送信する
- ホストが Linux ベースのオペレーティング システムを実行している

NAC 2.0 に関連する CTA のドキュメントには次のものがあります。

- Cisco Trust Agent 製品ページ
- Cisco Trust Agent リリース ノート V.2.0
- Cisco Trust Agent アドミニストレータ ガイド V.2.0

追加された NAC 対応コンポーネント

エンドポイントには、NAC コンポーネントとやり取りするアプリケーションがインストールされている場合があります。このようなアプリケーションは、追加された NAC インフラストラクチャを必要としたり、NAC を正常に機能させるために特別の設定を必要としたりすることがあります。

CSA に関するドキュメンテーション

Cisco Security Agent（CSA）は、組み込み型の分散セキュリティを企業に提供します。このセキュリティは、ネットワークやシステム全体を攻撃から保護するエージェントを配置することで実現されます。CSA は、ネットワーク管理者によってシステム ノードに選択的に割当てられた一連のポリシーを適用します。

CSA は独自のポスチャ プラグインを装備しており、要求されると CTA にポスチャ クレデンシャルを送信できます。

NAC 2.0 は、CSA バージョン 4.5.1.639、および 5.0.0.176 またはそれ以降でサポートされています。

- Cisco Security Agent 製品ページ
- Management Center for Cisco Security Agents V.4.5.1 リリース ノート
- Management Center for Cisco Security Agents V.4.5.1 のインストール
- Management Center for Cisco Security Agents V.4.5.1 の使用
- Policy Descriptions for CSA 4.5.1（Policy Descriptions を入手するには、Cisco.com へのユーザ登録が必要です）
- Management Center for Cisco Security Agents 5.0 リリース ノート
- Management Center for Cisco Security Agents 5.0 のインストール
- Management Center for Cisco Security Agents 5.0 の使用

Cisco Secure Monitoring Analysis and Response Systems（CS-MARS）

Cisco Secure Monitoring Analysis and Response Systems（CS-MARS）は、攻撃への対応、監視、被害の拡散防止のためのハイ パフォーマンスでスケーラブルなアプライアンスです。ネットワーク インテリジェンス、コンテキストの相関分析、ベクトル分析、異常検出、ホットスポット識別、および被害拡散防止の自動化機能が統合された CS-MARS により、ネットワークおよびセキュリティ デバイスをより効率的に使用することができます。

次のドキュメントには、CS-MARS と通信するための NAC デバイスおよびアプリケーションの設定方法が記載されています。

- Cisco Security Monitoring, Analysis and Response System 製品ページ
- Cisco Security Monitoring, Analysis and Response System 4.1