Cisco Secure Access Control System 5.8.1 インストレーション/アップグレード ガイド

2016 年 11 月

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

FCC クラス A 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述：このマニュアルに記載された装置は、無線周波エネルギーを生成および放射する可能性があります。シスコの指示する設置手順に従って設置されなかった場合、ラジオ、テレビによる受信障害が発生することがあります。この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの仕様は、住宅地で使用したときに、このような干渉を防止する適切な保護を規定したものです。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。

シスコの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に準拠しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

装置の電源を切ることによって、この装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコの装置またはその周辺機器が干渉の原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

・干渉がなくなるまで、テレビまたはラジオのアンテナの向きを変えます。

・テレビまたはラジオの左右どちらかの側に装置を移動させます。

・テレビまたはラジオから離れたところに装置を移動させます。

・テレビまたはラジオとは別の回路にあるコンセントに装置を接続します（装置とテレビまたはラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Copyright ©2005-2016 Cisco Systems, Inc. All rights reserved.

はじめに

改訂：２０１６年１１月３０日

このマニュアルでは、Cisco Secure Access Control System リリース 5.8.1（ACS 5.8.1）のシステム要件、インストール、アップグレード、設定、トラブルシューティング、およびメンテナンスのプロセスについて説明します。

ACS 5.8.1 は、ACS 5.8.1 サーバ、Cisco Application Deployment Engine オペレーティング システム リリース：2.2、ADE-OS ビルド バージョン：2.2.3.002、ADE-OS System Architecture：x86_64（Copyright (c) 2005-2016 by Cisco Systems, Inc. All rights reserved）と ACS 5.8.1 ソフトウェアで構成されます。

ADE-OS および ACS 5.8.1 ソフトウェアは、専用の SNS-3515、SNS-3595、SNS-3415、または SNS-3495 Access Control System シリーズ アプライアンス（Cisco SNS-3515、Cisco SNS-3595、Cisco SNS-3415 または Cisco SNS-3495）、専用の Cisco 1121 Secure Access Control System シリーズ アプライアンス（CSACS-1121）、または VMware サーバで実行されます。ただし、ACS 5.8.1 では、ACS 5.3 で使用した CSACS-1121 アプライアンスが引き続きサポートされます。ACS 5.3 または 5.4 から 5.8.1 に直接アップグレードすることはできません。ACS 5.3 または 5.4 は、5.5、5.6、5.7 または 5.8 にアップグレードする必要があります。ACS 5.5、5.6、5.7 または 5.8 は、ACS 5.8.1 に直接アップグレードできます。

仮想マシン（VM）ベースのインストールでは、最小のシステム要件を満たすように VM 環境を設定し、ACS 5.8.1 ソフトウェアをインストールする必要があります。サポートされる VMware バージョンは ESXi 5.0、5.1、5.5、6.0 です。

ACS 5.8.1 には、ADE-OS 2.x との互換性があります。ACS 5.1 を使用している場合は、ACS 5.8.1 のアップグレード時にこの ADE-OS バージョンにアップグレードする必要があります。

保証、サービス、およびサポート情報は、ご使用のアプライアンスに付属の『*Cisco Information Packet*』に含まれます。

対象読者

このマニュアルは、SNS-3515、SNS-3595、SNS-3415、SNS-3495、Cisco ACS 1121 アプライアンス、および VMware サーバをインストールおよび設定する管理者、ACS の導入をリリース 5.8.1 にアップグレードする管理者を対象としています。

このハードウェア マニュアルを使用するには、ネットワーク機器とケーブル接続についての知識と、電気回路と電気配線方法の基本的な知識が必要です。

警告：この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。ステートメント 1030

ガイドの構成

このマニュアルの内容は、概要、設置手順、アップグレード、インストール後の作業、およびリファレンス カテゴリにグループ分けされ、次のように分類されています。

表 1　ガイドの構成

パート	章
第 1 部：ACS サーバの導入	ACS サーバの導入について（1 ページ）：ACS サーバの導入とコンポーネントの概要が記載されています。新規の ACS 導入を計画するには、この章を参照してください。
第 2 部：Cisco 1121 Secure Access Control System 上の ACS 5.8.1	Cisco 1121 Secure Access Control System ハードウェアの導入（1 ページ）：CSACS-1121 ハードウェアの概要について説明します。
	Cisco 1121 Secure Access Control System ハードウェアの設置準備（1 ページ）：安全上の重要事項、設置場所の要件、および CSACS-1121 を設置する前に実行する作業について説明します。
	Cisco 1121 Secure Access Control System ハードウェアの設置（1 ページ）：ラック取り付け設定、CSACS-1121 のマウント、ケーブルの接続、アプライアンスの電源の投入、およびアプライアンスの取り外しと交換を行う手順について説明します。
	CSACS-1121 を使用した Cisco Secure Access Control System のインストールと設定（1 ページ）：CSACS-1121 を使用して ACS を新規にインストールする方法について説明します。
第 3 部：Cisco SNS 3400 サーバ上の ACS 5.8.1	Cisco SNS-3415 および Cisco SNS-3495 ハードウェア アプライアンスの導入（1 ページ）：Cisco SNS 3415 および Cisco SNS 3495 ハードウェアの概要を提供します。
	Cisco SNS 3415 および Cisco SNS 3495 ハードウェア アプライアンスの設置の準備（1 ページ）：安全上の重要事項、設置場所の要件、および Cisco SNS-3415 および Cisco SNS-3495 を設置する前に実行する作業について説明します。
	Cisco SNS 3415 および Cisco SNS 3495 ハードウェア アプライアンスの設置（1 ページ）：ラック取り付け設定、Cisco SNS-3415 および Cisco SNS-3495 のマウント、ケーブルの接続、アプライアンスの電源の投入、およびアプライアンスの取り外しと交換を行う手順について説明します。
	Cisco SNS-3415 および Cisco SNS-3495 を使用した Secure Access Control System のインストールと設定（1 ページ）：Cisco SNS-3415 および Cisco SNS-3495 を使用して ACS を新規にインストールする方法について説明します。
第 4 部：Cisco SNS 3500 サーバ上の ACS 5.8.1	Cisco SNS-3515 および Cisco SNS-3595 ハードウェア アプライアンスの導入（1 ページ）：Cisco SNS-3515 および Cisco SNS-3595 ハードウェアの概要を提供します。
	Cisco SNS 3515 および Cisco SNS 3595 ハードウェア アプライアンスの設置の準備（1 ページ）：安全上の重要事項、設置場所の要件、および Cisco SNS-3515 および Cisco SNS-3595 を設置する前に実行する作業について説明します。
	Cisco SNS 3515 および Cisco SNS 3595 ハードウェア アプライアンスの設置（1 ページ）：ラック取り付け設定、Cisco SNS-3515 および Cisco SNS-3595 のマウント、ケーブルの接続、アプライアンスの電源の投入、およびアプライアンスの取り外しと交換を行う手順について説明します。
	Cisco SNS-3515 および Cisco SNS-3595 を使用した Secure Access Control System のインストールと設定（1 ページ）：Cisco SNS-3515 および Cisco SNS-3595 を使用して ACS を新規にインストールする方法について説明します。

表 1　ガイドの構成（続き）

パート	章
第 5 部：VMware 仮想マシン上の ACS 5.8.1	VMware 仮想マシンへの ACS のインストール（1 ページ）：VMware ESX を使用した ACS のインストール方法について説明します。
第 6 部：リリース 5.8.1 への ACS のアップグレード	Cisco Secure Access Control システムのアップグレード（1 ページ）：ACS サーバを 5.5、5.6、5.7 または 5.8 から 5.8.1 にアップグレードする方法、および ACS 5.5、5.6、5.7 または 5.8 の導入を 5.8 にアップグレードする方法について説明します。
第 7 部：インストール後の作業	インストール後のタスク（1 ページ）：ACS ライセンスのインストールについて説明し、インストール後に実行する設定作業のリストを示します。
第 8 部：参考資料	トラブルシューティング（1 ページ）：CSACS-1121 の初期セットアップをトラブルシューティングするための方法について説明します。
	サイト ログ（1 ページ）：CSACS-1121、Cisco SNS-3415、Cisco SNS-3495、Cisco SNS-3515、または Cisco SNS-3595 のインストールと保守に関連するすべてのアクションを記録するサイト ログを維持するための推奨事項について説明します。
	CSACS-1121、Cisco SNS-3400 シリーズ、および Cisco SNS-3500 シリーズ アプライアンスの保守（1 ページ）：インストール後の CSACS-1121、Cisco SNS-3415、Cisco SNS-3495、Cisco SNS-3515 および Cisco SNS-3595 シリーズ アプライアンスの保守に対する推奨事項を提供します。

インストール、アップグレード、および移行のシナリオ

表 2（3 ページ）に、ACS 5.8.1 のインストール、アップグレード、または移行で遭遇する可能性がある一般的なシナリオを記載しています。シナリオごとに、それぞれの章またはマニュアルの参照先が、たどる必要がある順序で示されています。

表 2　インストール、アップグレード、および移行のシナリオ

シナリオ	参照
CSACS-1121 アプライアンスを使用した ACS の新規インストール	1. Cisco 1121 Secure Access Control System ハードウェアの導入（1 ページ） 2. Cisco 1121 Secure Access Control System ハードウェアの設置準備（1 ページ） 3. Cisco 1121 Secure Access Control System ハードウェアの設置（1 ページ） 4. CSACS-1121 を使用した Cisco Secure Access Control System のインストールと設定（1 ページ） 5. インストール後のタスク（1 ページ）

表 2　インストール、アップグレード、および移行のシナリオ（続き）

シナリオ	参照
Cisco SNS-3415 または Cisco SNS-3495 アプライアンスを使用した ACS の新規インストール	1. Cisco SNS-3415 および Cisco SNS-3495 ハードウェア アプライアンスの導入（1 ページ） 2. Cisco SNS 3415 および Cisco SNS 3495 ハードウェア アプライアンスの設置の準備（1 ページ） 3. Cisco SNS 3415 および Cisco SNS 3495 ハードウェア アプライアンスの設置（1 ページ） 4. Cisco SNS-3415 および Cisco SNS-3495 を使用した Secure Access Control System のインストールと設定（1 ページ） 5. インストール後のタスク（1 ページ）
Cisco SNS-3515 または Cisco SNS-3595 アプライアンスを使用した ACS の新規インストール	1. Cisco SNS-3515 および Cisco SNS-3595 ハードウェア アプライアンスの導入（1 ページ） 2. Cisco SNS 3515 および Cisco SNS 3595 ハードウェア アプライアンスの設置の準備（1 ページ） 3. Cisco SNS 3515 および Cisco SNS 3595 ハードウェア アプライアンスの設置（1 ページ） 4. Cisco SNS-3515 および Cisco SNS-3595 を使用した Secure Access Control System のインストールと設定（1 ページ） 5. インストール後のタスク（1 ページ）
VMware サーバを使用した ACS の新規インストール	1. VMware 仮想マシンへの ACS のインストール（1 ページ） 2. インストール後のタスク（1 ページ）
ACS 5.5、5.6、5.7、5.8 から 5.8.1 へのアップグレード	1. Cisco Secure Access Control システムのアップグレード（1 ページ）
同じハードウェア プラットフォーム（CSACS-1121 シリーズ アプライアンス）での ACS 4.2 からの移行	1. CSACS-1121 シリーズ アプライアンスから ACS 4.2 データをバックアップして、中間移行マシンでデータを復元します。 この中間移行マシンは Windows サーバでなければなりません。次の URL にある『ACS 5.8.1 Migration Guide』を参照してください。 http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-6/migration/guide/migration_guide.html 2. CSACS-1121 アプライアンスで ACS 5.8.1 のクリーン インストールを実行します。ACS サーバの再イメージ化（6 ページ）を参照してください 3. 『ACS 5.8.1 Migration Guide』に記載されている指示に従って、ACS 4.2 から ACS 5.8.1 へのデータの移行を実行します。参照先： http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-6/migration/guide/migration_guide.html

表 2　インストール、アップグレード、および移行のシナリオ（続き）

シナリオ	参照
別のハードウェア プラットフォームでの ACS 4.2 からの移行	1. CSACS-1121、Cisco SNS 3400、または Cisco SNS 3500 シリーズ アプライアンスまたは VMware サーバで ACS 5.8.1 の初期インストールを実行します。 – CSACS-1121 アプライアンスに ACS 5.8.1 をインストールするには、CSACS-1121 シリーズ アプライアンスを使用したインストール（1 ページ）を参照してください。 – Cisco SNS 3400 シリーズ アプライアンスに ACS 5.8.1 をインストールするには、Cisco SNS-3415/3495 アプライアンスへの ACS のインストール（1 ページ）を参照してください。 – Cisco SNS 3500 シリーズ アプライアンスに ACS 5.8.1 をインストールするには、Cisco SNS-3515/3595 アプライアンスへの ACS のインストール（1 ページ）を参照してください。 – VMware サーバに ACS 5.8.1 をインストールするには、VMware 仮想マシンへの ACS のインストール（1 ページ）を参照してください。 2. 『ACS 5.8.1 Migration Guide』に記載されている指示に従って、ACS 4.2 から ACS 5.8.1 へのデータの移行を実行します。参照先: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-6/migration/guide/migration_guide.html

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。

項目	表記法
手順で選択する必要があるコマンド、キーワード、特殊な用語、およびオプション	**太字**
ユーザが値を指定する変数、および新しい用語や重要な用語	*italic* フォント
セッション情報、システム情報、パス、およびファイル名の表示出力	`screen` フォント
ユーザが入力する情報	**太字の `screen` フォント**
ユーザが入力する変数	*イタリック体の `screen` フォント*
メニュー項目およびボタン名	[ ]
メニュー項目の選択順序	**[オプション（Option）] > [ネットワーク設定（Network Preferences）]**

注: *読者に留意していただきたいこと*を示しています。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: ***注意が必要なこと*を示します。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。**

安全上の警告

誤って行うと危険が生じる可能性のある操作については、安全上の警告が記載されています。各警告文には、警告を表す記号が記されています。安全上の警告は、電源または電話回線に接続する機器を取り扱う際に従う必要がある安全に関する推奨事項を提供します。警告の各国語版があります。

コンプライアンスのガイドラインと安全上に警告の翻訳文については、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を参照してください。

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. sUtilizzare 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**

製品に関する資料

注:印刷ドキュメントと電子ドキュメントは初版発行後に更新されることがあります。マニュアルの更新については、http://cisco.com で確認してください。

表 3（10 ページ） に、Cisco.com で入手可能な ACS 5.8.1 の製品マニュアルを示します。Cisco.com ですべての製品のエンドユーザ向けマニュアルを検索するには、http://www.cisco.com/go/techdocs に移動してください。

[Products] > [Security] > [Access Control and Policy] > [Secure Access Control System] > [Cisco Secure Access Control System 5.8.1] の順に選択します。

表 3　製品に関する資料

参照先	利用可能なフォーマット
『Cisco Secure Access Control System In-Box Documentation and China RoHS Pointer Card』	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-documentation-roadmaps-list.html
『Migration Guide for Cisco Secure Access Control System 5.8.1』	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
『User Guide for Cisco Secure Access Control System 5.8.1』	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html
『CLI Reference Guide for Cisco Secure Access Control System 5.8.1』	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-command-reference-list.html
『Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.8.1』	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-device-support-tables-list.html
『Release Notes for Cisco Secure Access Control System 5.8.1』	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-release-notes-list.html

表 3　製品に関する資料（続き）

参照先	利用可能なフォーマット
『Software Developer's Guide for Cisco Secure Access Control System 5.8.1』	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-programming-reference-guides-list.html
『Regulatory Compliance and Safety Information for Cisco Secure Access Control System』	http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-4/regulatory/compliance/csacsrcsi.html

マニュアルの更新

表 4（11 ページ）に、『Cisco Secure Access Control System 5.8.1 インストレーション/アップグレード ガイド』の更新内容を示します。

表 4　『Cisco Secure Access Control System 5.8.1 インストレーション/アップグレード ガイド』の更新

日付（Date）	説明
2016 年 3 月 21 日	Cisco Secure Access Control System、リリース 5.8.1

マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool（BST）の使用法、サービス要求の送信、および追加情報の収集方法については、「*What's New in Cisco Product Documentation*」（http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html）を参照してください。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、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、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

マニュアルの更新

ACS サーバの導入

ACS サーバの導入について

この章では、ACS サーバの考えられる導入方法とそのコンポーネントの概要について説明します。

この章の内容は、次のとおりです。

- 導入シナリオ（1 ページ）
- ACS サーバの設定について（4 ページ）

導入シナリオ

ここでは、ACS を使用する次の 3 つの導入シナリオについて説明します。

- 小規模 ACS 導入（1 ページ）
- 中規模 ACS 導入（2 ページ）
- 大規模 ACS 導入（3 ページ）

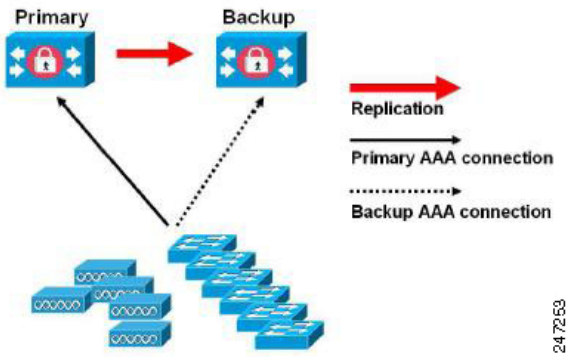
小規模 ACS 導入

最も基本的な ACS の導入は、図 1（1 ページ）に示すように、2 台のサーバで構成されます。第 1 のサーバは、ネットワークのすべての設定、認証、ポリシー要件を満たすプライマリ サーバです。

第 2 のサーバは、AAA クライアントとプライマリ サーバ間の接続が失われた場合にバックアップ サーバとして使用されます。プライマリ ACS サーバからセカンダリ サーバへのレプリケーションを使用して、セカンダリ サーバがプライマリ サーバと同期している状態を保ちます。

小規模なネットワークでは、この構成により、プライマリとセカンダリの RADIUS または TACACS サーバを、すべての AAA クライアントで同じように設定できます。

図 1　小規模 ACS 導入



組織内のユーザと AAA クライアントの数の増加に応じて、ACS の導入方法を基本的な設計から変更し、図 2（2 ページ）に示す分割 ACS 導入設計を使用することを推奨します。

分割 ACS 導入

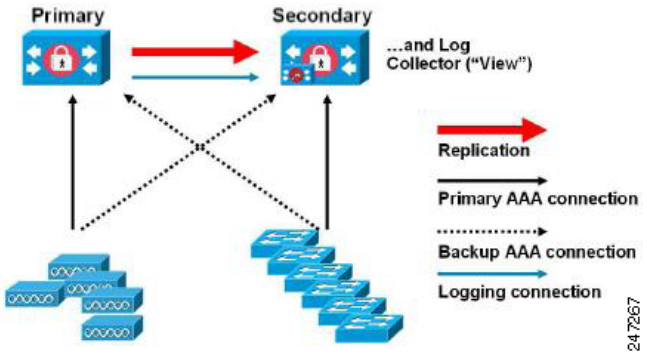
分割 ACS 導入では、小規模 ACS 導入と同様にプライマリ サーバとセカンダリ サーバを使用しますが、AAA の負荷を 2 台のサーバに分散し、AAA フローを最適化します。AAA 接続に問題が発生した場合は、各サーバが両方のサーバのすべての負荷を処理しますが、通常運用時には、どちらのサーバも認証要求のすべての負荷を処理することはありません。

サーバのこの特性により、各 ACS システムへの負荷が最適化され、通常運用の中でセカンダリ サーバの動作状況を知ることができます。

この配置のもう 1 つの利点は、各サーバをデバイスの管理やネットワークの許可など特定の運用のために使用しながら、障害時にすべての AAA 機能を実行できることです。

2 台の ACS システムが、AAA クライアントからの認証要求の処理とアカウンティング データの収集を行うため、一方のシステムをログ コレクタとして使用することを推奨します。図 2（2 ページ）では、セカンダリ ACS サーバをログ コレクタとして使用しています。

図 2　分割 ACS 導入

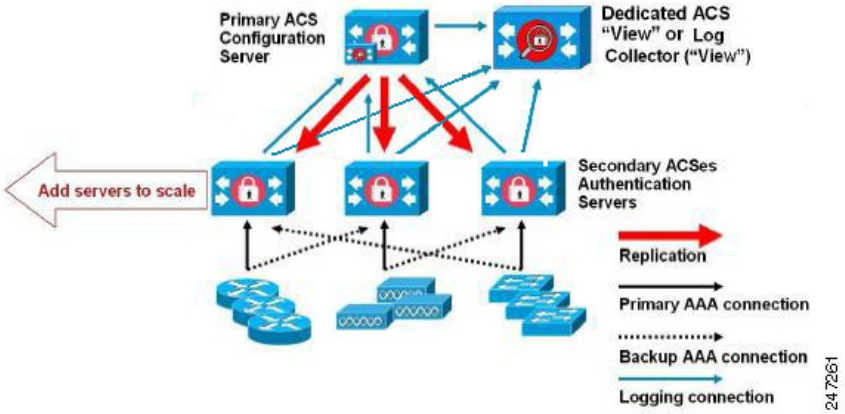


この設計のもう 1 つの利点は、図 3（3 ページ）に示すように拡張が可能なことです。

中規模 ACS 導入

ローカル ネットワークの成長に応じて、さらに ACS サーバをシステムに追加する必要があります。このシナリオでは、プライマリ サーバを昇格させて構成サービスを実行し、AAA 機能をセカンダリ サーバで使用することを検討します。ログ トラフィック量が増大した場合は、セカンダリ サーバの 1 台を専用の中央ログ コレクタ サーバとして使用する必要があります。ACS 5.8.1 は、導入への ACS インスタンス 1 個の追加をサポートします。ACS 5.8.1 中規模導入は 14 個の ACS インスタンスをサポートします。実際のプライマリ インスタンスを降格させる場合に、この追加 ACS インスタンスをプライマリ インスタンスにプロモート可能な専用インスタンスとして指定できます。

図 3　中規模 ACS 導入



大規模 ACS 導入

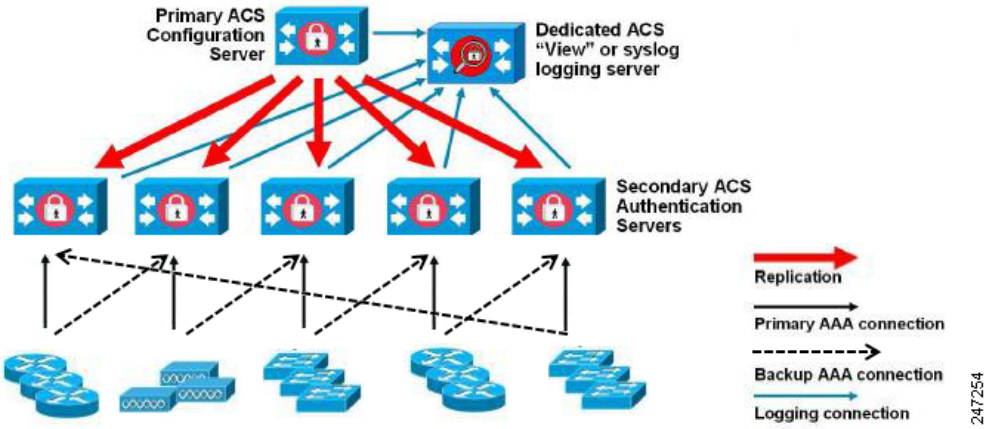
図 4（3 ページ）に示すような大規模 ACS 導入では、集中ロギングの使用を強く推奨します。ACS 5.8.1 は、導入への ACS インスタンス 1 個の追加をサポートします。ACS 5.8.1 大規模導入は 22 個の ACS インスタンスをサポートします。実際のプライマリ インスタンスを降格させる場合に、この追加 ACS インスタンスをプライマリ インスタンスにプロモート可能な専用インスタンスとして指定できます。使用率の高いネットワークでは、大量の syslog トラフィックが生成される可能性があるため、専用のロギング サーバ（モニタリングおよびレポート サーバ）のを推奨します。ACS は発信ログ トラフィックに対して syslog メッセージを生成するため、RFC-3164 に準拠した任意の syslog サーバを使用して発信ロギング トラフィックを収集できます。

このタイプのサーバでは、すべての ACS サーバに対して、ACS が備えているレポート機能とアラート機能を使用できます。これには特別なライセンスが必要です（『User Guide for Cisco Secure Access Control System 5.8.1』を参照してください）。ACS サーバのインストールの詳細については、ACS サーバのインストール（2 ページ）を参照してください。

モニタリングおよびレポートサーバと汎用 syslog サーバの両方にログを送信するようにサーバを設定することも検討してください。汎用 syslog サーバを追加することにより、モニタリングおよびレポート サーバがダウンした場合に、バックアップが提供されます。

注：ACS 5.8.1 は、ACS インスタンス数が 22 を超える大規模導入をサポートしていません。

図 4　大規模 ACS 導入



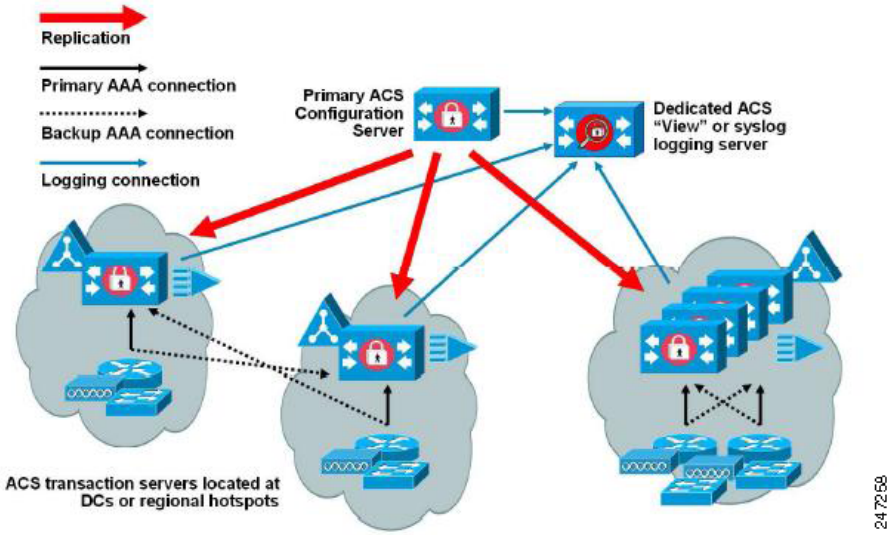
分散 ACS 導入

分散 ACS 導入は、世界中にキャンパスがある組織で有効です。ホーム キャンパスにプライマリ ネットワークがある場合もありますが、さまざまな地域のキャンパスに、小規模から大規模の LAN が存在することもあります。

AAA パフォーマンスを最適化するために、これらの各リモート キャンパスには独自の AAA インフラストラクチャを配置します。図 5（4 ページ）を参照してください。一貫性のある同期された AAA ポリシーを維持するためには、中央管理モデルを使用する必要があります。

集中化された構成でも、プライマリ ACS サーバと個別のモニタリングおよびレポート サーバを使用する必要があります。ただし、各リモート キャンパスには固有の要件があります。

図 5　分散 ACS 導入



リモート サイトがあるネットワークを計画する際に検討すべき要素としては、次のものがあります。

- 中央または外部データベース（Microsoft Active Directory（AD）または Lightweight Directory Access Protocol（LDAP））を使用しているかどうかを確認します。最適化のために、ACS がアクセス可能な、外部データベースの同期されたインスタンスを各リモート サイトに配置する必要があります。
- AAA クライアントの場所も重要な留意事項です。ネットワークの遅延による影響や、WAN 障害によってアクセスできなくなる可能性を減らすために、ACS サーバは、できるだけ AAA クライアントの近くに配置する必要があります。
- ACS では、バックアップなどの一部の機能にコンソールからアクセスできます。各サイトで端末を使用することを検討します。これにより、ネットワークの外部から各サーバに対するセキュアなコンソール アクセスが可能になります。
- 小規模なリモート サイトが近くにあり、他のサイトへの信頼できる WAN 接続がある場合は、近くのサイトにある ACS サーバをローカル サイトのバックアップ サーバとして使用し、冗長性のある構成とすることもできます。
- 外部データベースにアクセスできるようにするには、すべての ACS ノードで DNS を適切に設定する必要があります。

ACS サーバの設定について

ここでは、各種 ACS サーバの役割と、その設定方法についての概要を説明します。ロールのサーバへの割り当てと設定の詳細については、『*User Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。

ここでは、次の項目について説明します。

- プライマリ サーバ(5 ページ)
- セカンダリ サーバ(5 ページ)
- ロギング サーバ(6 ページ)

インストール手順は、どの ACS サーバでも同様です。

CSACS-1121 アプライアンスを使用した ACS のインストールについては、CSACS-1121 を使用した Cisco Secure Access Control System のインストールと設定(1 ページ)を参照してください。Cisco SNS 3400 シリーズ アプライアンスを使用した ACS のインストールについては、Cisco SNS-3415 および Cisco SNS-3495 を使用した Secure Access Control System のインストールと設定(1 ページ)を参照してください。Cisco SNS 3500 シリーズ アプライアンスを使用した ACS のインストールについては、Cisco SNS-3415 および Cisco SNS-3495 を使用した Secure Access Control System のインストールと設定(1 ページ)を参照してください。VMware ESX を使用した ACS のインストールについては、VMware 仮想マシンへの ACS のインストール(1 ページ)を参照してください。ACS 導入では、最初に必ずプライマリ サーバをインストールしてください。

プライマリ サーバ

ACS 導入では、1 つのインスタンスだけが ACS プライマリとなり、構成機能を提供するとともに、レプリケーションのソースとなります。

ACS プライマリ サーバでは、ACS の導入に必要なすべてのシステム設定を行うことができます。ただし、ライセンスとローカル証明書は、各 ACS セカンダリ サーバで個別に設定する必要があります。

セカンダリ サーバ

プライマリ サーバを除く他のすべてのインスタンスはセカンダリ サーバとして機能します。

セカンダリ ACS サーバは、プライマリ サーバからすべてのシステム設定を受け取ります。ただし、次のものは各セカンダリ サーバで設定する必要があります。

- ライセンス:導入内の各 ACS セカンダリ サーバに対し、固有の基本ライセンスをインストールします。
- 新しいローカル証明書:セカンダリ サーバでローカル証明書を設定するか、プライマリ サーバからローカル証明書をインポートします。
- ログ収集サーバ:プライマリ サーバとセカンダリ サーバのいずれかを、ACS のログ収集サーバとして設定できます。セカンダリ ACS サーバをロギング サーバとして設定することを推奨します。

注: セカンダリ サーバのインストール先を選択する場合、プライマリ サーバとセカンダリ サーバの間でネットワーク アドレスは変換できません。

セカンダリ サーバを ACS 環境の一部とするためには、アクティベーションを行う必要があります。管理者は、セカンダリ サーバのアクティベーションを行うか、自動アクティベーションを設定する必要があります。デフォルトでは、アクティベーションは自動に設定されます。

セカンダリ サーバは、アクティベーションが行われると、設定とレプリケーションの更新がプライマリ サーバと同期されます。

ロギング サーバ

プライマリ サーバまたはいずれかのセカンダリ サーバがロギング サーバとして機能できます。

ロギング サーバは、導入内のプライマリ サーバとすべての ACS セカンダリ サーバからログを受信します。ACS セカンダリ サーバのうちの 1 台をモニタリングおよびレポート サーバとして割り当て、このセカンダリ サーバを AAA アクティビティから除外することを推奨します。

3 つの主なロギング カテゴリは、監査、アカウンティング、および診断です。

ロギング カテゴリと設定の詳細については、『*User Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。

Cisco 1121 Secure Access Control System 上の ACS 5.8.1

Cisco 1121 Secure Access Control System ハードウェアの導入

この章では、Cisco Secure Access Control System（CSACS-1121）ハードウェアの概要を紹介します。ここでは、アプライアンス ハードウェア、主なコンポーネント、コントロール、コネクタ、前面および背面パネルの LED インジケータについて説明します。

この章の内容は、次のとおりです。

- 製品の概要（1 ページ）
- ハードウェアの機能（3 ページ）
- 法規制の遵守（6 ページ）

製品の概要

この項では、CSACS-1121 シリーズ アプライアンスの電源要件、ラックマウント ハードウェア キット、および機能について説明します。

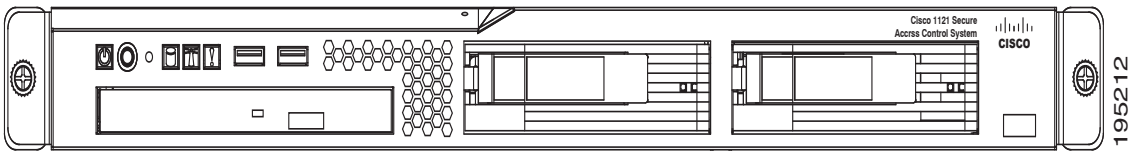
ここでは、次の項目について説明します。

- CSACS-1121 シリーズ アプライアンスの概要（1 ページ）
- 製品シリアル番号の場所（2 ページ）
- Cisco Product Identification ツール（3 ページ）

CSACS-1121 シリーズ アプライアンスの概要

CSACS-1121 シリーズ アプライアンス（図 1（1 ページ）を参照）は、標準シェルフのラック キャビネットに格納されます。このアプライアンスの重さは、24.25 ～ 28.0 ポンド（11.0 kg ～ 12.7 kg）です。寸法は、高さ 1.75 インチ X 幅 17.3 インチ X 奥行 22.0 インチ（44.5 mm X 440.0 mm X 559.0 mm）です。これらの寸法は、ラック ハンドルを含みません。

図 1　Cisco 1121 Secure Access Control System 正面図



CSACS-1121 シリーズ アプライアンスは AC 入力電源を使用するように設定されており、1 個のオートレンジ AC 入力電源が標準の 19 インチ（48.3 cm）、4 支柱装置ラックに（付属のラック取り付け金具で）取り付けられています。CSACS-1121 の機能は、次のとおりです。

- マイクロプロセッサ。800-MHz の Front Side Bus（FSB; フロント サイド バス）および 2 MB のレイヤ 2 キャッシュの Intel Core 2 Duo 2.4-GHz プロセッサ。
- 4 GB インストールの同期ダイナミック RAM（SDRAM）4 スロット。

- 250 GB SATA ハード ドライブ 2 台（インストール済み）。
- 固定 RJ-45 10BASE-T/100BASE-TX/1000BASE-T ネットワーク インターフェイス コネクタ（背面パネルに配置）。
- スリムライン DVD-ROM ドライブ 1 台（前面パネルに配置）。
- DB-9 シリアル（コンソール）ポート 1 個（背面パネルに配置）。
- 前面から背面に向けた通気ブロアー。CPU およびメモリ用の 40 mm 排気ファンおよびダクト 2 枚と、電源内に組み込まれた 40 mm 排気ファン 2 枚、および PCI 排気ファン 1 枚を使用。
- 拡張スロットのサポート。PCI-X（背面パネルに配置）1 つ。
- USB 2.0 ポート 4 個（背面パネルに 2 個、前面パネルに 2 個）。
- PS/2 キーボード ポート 1 個（背面パネルに配置）。
- PS/2 マウス ポート 1 個（背面パネルに配置）。
- PS/2 ビデオ モニタリング ポート 1 個（背面パネルに配置）。
- DB-15 シリアル（ビデオ）ポート 1 個（背面パネルに配置）。
- 4 ギガビット イーサネット インターフェイス。
- 背面アクセス式ケーブル。
- アプライアンスの前面パネル LED：
  - アプライアンス電源
  - ハードディスク ドライブ アクティビティ
  - ロケータ
  - システム エラー（System error）
  - CD ドライブ アクティビティ

  LED の詳細については、CSACS-1121 アプライアンスの前面パネル図（4 ページ）を参照してください。
- アプライアンスの背面パネル LED：
  - イーサネット アクティビティ
  - イーサネット リンク

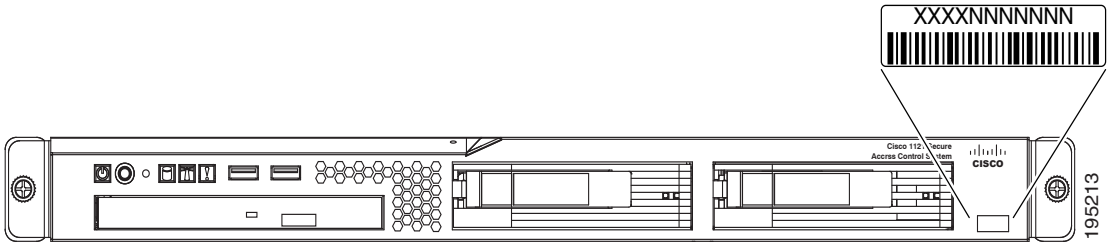
  LED の詳細については、CSACS-1121 アプライアンスの背面パネル図（5 ページ）を参照してください。
- 通常、CSACS-1121 アプライアンスは CSACS-1121 を 4 支柱装置ラック内に配置するためのブラケットまたはラックを含むラックマウント ハードウェア キットとともに出荷されます。詳細については、Cisco 1121 Secure Access Control System ハードウェアの設置（1 ページ）を参照してください。

  注：ラックマウント ハードウェア キットに 2 支柱装置ラックは含まれていません。

製品シリアル番号の場所

CSACS-1121 シリーズ アプライアンスのシリアル番号ラベルは、アプライアンスの前面パネルの左下にあります。図 2（3 ページ）に、このラベルの場所を示します。

図 2　CSACS-1121 アプライアンスのシリアル番号の場所



注:CSACS-1121 シリーズ アプライアンスのシリアル番号は 11 文字です。

Cisco Product Identification ツール

Cisco 製品 ID(CPI)ツールは、シスコ製品のシリアル番号を取得する際に役立ちます。

オンラインまたは電話でサービスのリクエスト要求をする前に、CPI ツールを使用して製品のシリアル番号を検索します。このツールは、シスコのサポート Web サイトからアクセスできます。

ツールにアクセスする方法は、次のとおりです。

1. [Get Tools & Resources] リンクをクリックします。
2. [All Tools (A-Z)] タブをクリックします。
3. アルファベット順のドロップダウン リストから [Cisco Product Identification Tool] を選択します。

   このツールには、3 つの検索オプションがあります。

- 製品 ID またはモデル名による検索。
- シスコ モデルの参照。
- **show** コマンドで出力をコピー アンド ペーストして製品を特定。

  検索結果では、製品画像とともにシリアル番号ラベルの場所が強調表示されます。製品のシリアル番号ラベルのある場所を探し、サービスに問い合わせる前にその情報を記録します。

  CPI ツールは、次の URL からアクセスできます。

  http://tools.cisco.com/Support/CPI/index.do

  CPI ツールにアクセスするには、Cisco.com ユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

  http://tools.cisco.com/RPF/register/register.do

ハードウェアの機能

この項では、CSACS-1121 シリーズ アプライアンスの前面および背面パネルのコントロール、ポート、および LED インジケータについて説明します。

ここでは、次の項目について説明します。

- CSACS-1121 アプライアンスの前面パネル図(4 ページ)
- CSACS-1121 アプライアンスの背面パネル図(5 ページ)
- 入力/出力ポートおよびコネクタ(6 ページ)

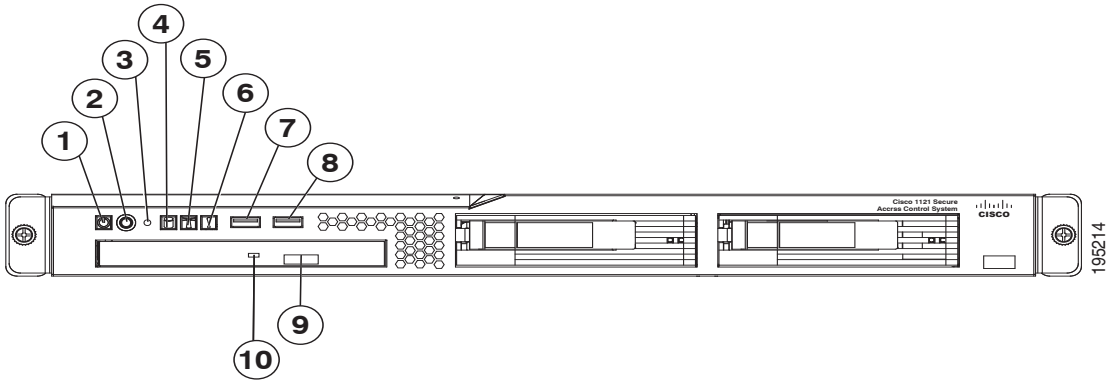
CSACS-1121 アプライアンスの前面パネル図

CSACS-1121 シリーズ アプライアンスの前面パネルは、次のとおりに構成されます。

- 電源制御ボタン
- リセットボタン
- USB 2.0 ポート 2 個
- CD 取り出しボタン
- 各種 LED（アプライアンスおよび CD ドライブ）

図 3（4 ページ） に、前面パネルのコンポーネントを示します。

図 3　CSACS-1121 シリーズ アプライアンスの正面図



次の表で、図 3（4 ページ） の各コンポーネントについて説明します。

1	アプライアンス電源 LED	6	システム エラー LED
2	電源制御ボタン	7	USB 1 コネクタ
3	リセットボタン	8	USB 2 コネクタ
4	ハードディスク ドライブ アクティビティ LED	9	CD 取り出しボタン
5	ロケータ LED	10	CD ドライブ アクティビティ LED

CSACS-1121 前面パネルの LED

表 1（4 ページ） で、CSACS-1121 シリーズ アプライアンスの前面パネルに配置された LED について説明します。

表 1　前面パネルの LED

LED	カラー	状態	説明
アプライアンス電源	グリーン	オン	電源オン
	グリーン	点滅	スリープ（スタンバイ）
	オフ	オフ	電源オフ
ハード ディスク ドライブ	グリーン	ランダムに点滅	ハードディスク ドライブ アクティビティ
	オフ	オフ	ハードディスク ドライブ アクティビティなし

表 1　前面パネルの LED（続き）

LED	カラー	状態	説明
リセットボタン	–	–	このボタンを押してソフト リセットを実行
ロケータ LED	青	点滅	システムの起動中
	オフ	オフ	システムの起動完了
システム エラー	オレンジ	オン	システム エラー発生
CD ドライブ アクティビティ	グリーン	オン	CD ドライブ使用中

CSACS-1121 アプライアンスの背面パネル図

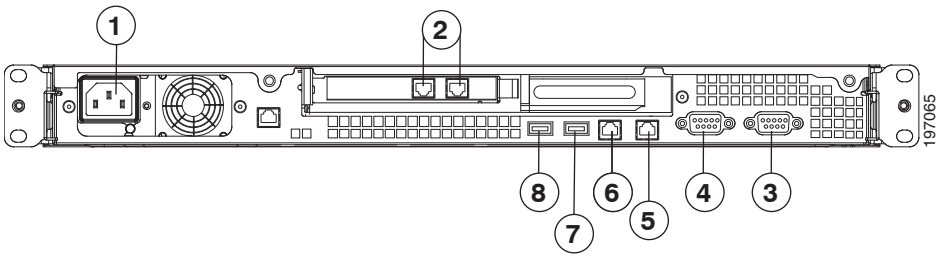
CSACS-1121 シリーズ アプライアンスの背面パネルは、次のとおりに構成されます。

- AC 電源コネクタ
- シリアル コネクタ
- ビデオ コネクタ 1 個
- イーサネット（RJ-45）コネクタ 4 個
- USB 2.0 ポート 2 個
- イーサネット LED

図 4（5 ページ） に、背面パネルのコンポーネントを示します。

ラックマウント ブラケットの場所も、アプライアンスの左横および右横に示します（マウント ブラケットのインストール方法については、ラックマウント構成のガイドライン（1 ページ）を参照してください）。

図 4　CSACS-1121 シリーズ アプライアンスの背面図



次の表で、図 4（5 ページ） の各コンポーネントについて説明します。

1	AC 電源コンセント	5	ギガビット イーサネット 1
2	ギガビット イーサネット	6	（使用中）ギガビット イーサネット 0 **注**：ネットワークのインストールと管理インターフェイスには、この NIC を使う必要があります。
3	シリアル コネクタ	7	USB 3 コネクタ
4	ビデオ コネクタ	8	USB 4 コネクタ

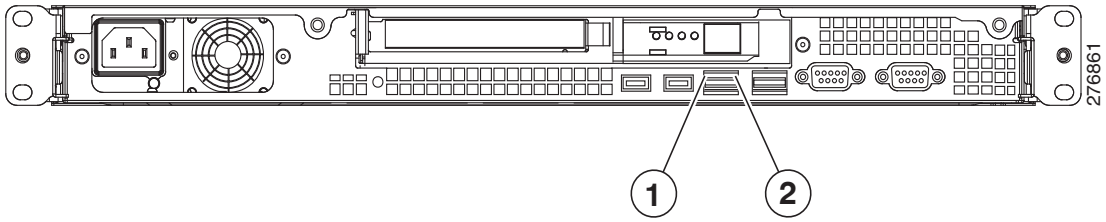
CSACS-1121 背面パネルの LED

表 2（6 ページ）で、CSACS-1121 シリーズ アプライアンスの背面パネルに配置された LED について説明します。図 5（6 ページ）に、これら LED を示します。

表 2　背面パネルの LED

LED	カラー	状態	説明
イーサネット アクティビティ LED	グリーン	オン	サーバとネットワーク間でアクティビティあり
	グリーン	点滅	サーバとネットワーク間でアクティビティあり
	オフ	オフ	アクティビティなし
イーサネット リンク LED	グリーン	ランダムに点滅	イーサネット コントローラがネットワークに接続中
	オフ	オフ	イーサネット コントローラがネットワークに非接続

図 5　CSACS-1121 の背面パネルの LED



入力/出力ポートおよびコネクタ

CSACS-1121 シリーズ アプライアンスは、次の入力/出力コネクタの種類をサポートします。

- ギガビット イーサネット ポート 2 個（背面パネル）
- シリアル ポート 1 個（背面パネル）
- パラレル ポート 1 個（背面パネル）
- USB 2.0 ポート（前面パネルに 2 個、背面パネルに 2 個）

警告：感電を防ぐために、安全超低電圧（SELV）回路を電話網電圧（TNV）回路に接続しないでください。LAN ポートには SELV 回路が、WAN ポートには TNV 回路が組み込まれています。一部の LAN ポートおよび WAN ポートでは、共に RJ-45 コネクタが使用されています。ケーブルを接続する際、注意してください。ステートメント 1021

法規制の遵守

法令準拠および安全性に関する情報については、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を参照してください。

詳細については、マニュアルの入手方法およびテクニカル サポート（11 ページ）を参照してください。

Cisco 1121 Secure Access Control System ハードウェアの設置準備

この章では、安全上の重要事項、設置場所の要件、および CSACS-1121 シリーズ アプライアンスを設置する前に実行する必要がある作業について説明します。

この章の内容は、次のとおりです。

- 安全に関するガイドライン（1 ページ）
- 設置場所の準備（5 ページ）
- イーサネットとコンソール ポートに関する考慮事項（13 ページ）

注：インストールを開始する前に、『*Regulatory Compliance and Safety Information for the Cisco 1121 Secure Access Control System*』を参照してください。

安全に関するガイドライン

CSACS-1121 シリーズ アプライアンスの設置を開始する前に、人身事故または装置の損傷を防ぐために、この章とラックマウント構成のガイドライン（1 ページ）に記載されている安全に関する推奨事項を確認してください。

さらに、アプライアンスの交換、構成、または保守を行う前に、安全上の警告（6 ページ）とマニュアル『*Cisco Regulatory Compliance and Safety Information for the Cisco 1121 Secure Access Control System*』に記載されている安全上の警告を参照してください。

ここでは、次の項目について説明します。

- 一般的な注意事項（1 ページ）
- 機器を扱う場合の注意（2 ページ）
- 電気製品を扱う場合の注意（3 ページ）
- 静電破壊の防止（4 ページ）
- 持ち上げ時の注意事項（5 ページ）

一般的な注意事項

アプライアンスの使用および取り扱いには、次の一般的な注意事項を守ってください。

- サービスに関するマーキングに従ってください。アプライアンス マニュアルで説明されている場合を除き、シスコ製品の保守を行わないでください。稲妻が示された三角形のシンボルのマークが付いたカバーを開けたり取り外したりすると、感電するおそれがあります。これらのコンパートメント内のコンポーネントの保守は、許可された保守技術者だけが行う必要があります。

- 次のいずれかの状態が発生した場合は、電源コンセントから製品を取り外してパーツを交換するか、認可された保守技術者にご連絡ください。
  - 電源ケーブル、延長コード、またはプラグが損傷している。
  - 何かの物体が製品に入り込んだ。
  - 製品に水がかかった。
  - 製品が落下または損傷した。
  - 操作指示に従っているのに、製品が正しく動作しない。
- アプライアンスをラジエータや熱源の近くに置かないでください。また、通気口をふさがないでください。
- アプライアンスの上に食べ物や液体をこぼさないでください。また、水気のある環境で本製品を操作しないでください。
- アプライアンスの開口部に物を押し込まないでください。内部コンポーネントがショートして火災や感電の原因となる可能性があります。
- 製品は、シスコによって承認されている他の機器だけで使用してください。
- カバーを取り外したり、内部コンポーネントに触れたりする場合は、製品が十分に冷えるまでお待ちください。
- 正しい外部電源を使用してください。製品は、電力定格ラベルに記載されている種類の電源だけを使用して稼働させてください。必要な電源の種類が不明な場合は、サービス担当者または現地の電力会社にお問い合わせください。
- 認定された電源ケーブルだけを使用してください。ご使用のアプライアンス用、またはご使用のアプライアンス向けの AC 電源オプション用の電源ケーブルが付属していない場合は、国で使用が承認された電源ケーブルを購入してください。

  電源ケーブルが、製品と、製品の電気定格ラベルに記載された電圧および電流に適合することを確認してください。電源ケーブルの電圧および定格電流は、製品に記載された定格を上回るものでなければなりません。
- 感電事故を予防するため、アプライアンスおよび電源ケーブルは、適正に接地されたコンセントに接続してください。これらのケーブルには適切な接地を可能にする 3 極プラグが装着されています。アダプタ プラグを使用したり、ケーブルから接地極を外したりしないでください。延長コードを使用する必要がある場合は、適切に接地されたプラグが装着された 3 線コードを使用してください。
- 延長コードとテーブル タップの定格を遵守してください。延長コードまたは電源ストリップに差し込まれているすべての製品の定格アンペアの合計が、延長コードまたは電源ストリップの定格アンペア制限の 80% を超えないことを確認してください。
- アプライアンス、電圧変換器、またはアプライアンス用に販売されているキットを製品と一緒に使用しないでください。
- 一時的に急激に起こる電源電圧の上昇または下降からアプライアンスを保護するには、サージ抑制装置、パワー コンディショナ、または無停電電源装置(UPS)を使用してください。
- ケーブルと電源コードは慎重に配置してください。ケーブルと電源コードは、人に踏まれたり、それによって人が躓くことがないように配線して差し込んでください。また、アプライアンスのケーブルまたは電源ケーブルの上に物を置かないように注意してください。
- 電源ケーブルとプラグを改造しないでください。場所を変更する場合は、ライセンスを待つ電気技術者または電力会社にお問い合わせください。現地または該当国の配線規定に必ず従ってください。

機器を扱う場合の注意

安全を確保して、機器を保護するため、次の注意事項に従ってください。ただし、このリストには、生じる可能性のある危険な状況がすべて網羅されているわけではありません。*注意を怠らないでください*。

警告:システムを電源に接続する前に設置の説明書をお読みください。ステートメント 1004

- アプライアンスを移動する前に、必ずすべての電源コードおよびインターフェイス ケーブルを外してください。
- 回路の電源が切断されていると思い込まないで、*必ず*確認してください。
- 設置作業前および作業後は、アプライアンスのシャーシの設置場所を整理し、埃のない状態に保ってください。
- 工具とアセンブリ コンポーネントは、通行の邪魔にならない場所に保管してください。
- 危険を伴う作業は、1 人では行わないでください。
- 人身事故や装置障害を引き起こす可能性のある作業は行わないでください。
- アプライアンスのシャーシに引っかかることがないよう、ゆったりとした衣服は身につけないでください。
- 目が危険にさらされる状況で作業する場合は、保護眼鏡を着用してください。

電気製品を扱う場合の注意

警告:この装置は、立ち入りが制限された場所への設置を前提としています。立ち入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段を使用しないと入室できない場所を意味します。ステートメント 1017

警告:感電を防ぐために、安全超低電圧(SELV)回路を電話網電圧(TNV)回路に接続しないでください。LAN ポートには SELV 回路が、WAN ポートには TNV 回路が組み込まれています。一部の LAN ポートおよび WAN ポートでは、共に RJ-45 コネクタが使用されています。ステートメント 1021

警告:電源コードが接続されている場合、電源に触れないでください。電源スイッチを備えたシステムの場合、電源スイッチがオフになっていても、電源コードが接続されていれば、電源装置内部に入力電圧がかかっています。電源スイッチのないシステムの場合、電源コードが接続されていれば、電源装置内部に入力電圧がかかっています。ステートメント 4

警告:電力系統に接続されている機器の作業を行う前に、宝飾品(指輪、ネックレス、腕時計を含む)を取り外してください。金属は電源やアースに接触すると、過熱して重度のやけどを引き起こしたり、金属類が端子に焼き付いたりすることがあります。ステートメント 43

警告:シャーシに対する作業や電源のそばでの作業の前に、AC ユニットの電源コードを取り外し、DC ユニットでは回路ブレーカーで電源を切断してください。ステートメント 12

警告:雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

警告:この装置は接地されることを前提としています。通常の使用時にホストが接地されていることを確認してください。ステートメント 39

警告:装置を設置または交換する際は、必ずアースを最初に接続し、最後に取り外します。ステートメント 1046

電気機器を取り扱う際には、次の注意事項に従ってください。

- 部屋の緊急電源切断スイッチを確認します。これにより、電気事故が発生した場合に、ただちに電源をオフにすることができます。
- 次の作業を行う前に、すべての電源をオフにしてください。
  - 電源付近で作業する場合。
  - アプライアンスの取り付けまたは取り外しを行う場合。
  - ほとんどのハードウェア アップグレードを行う場合。

- 故障していると思われる機器は取り付けないでください。
- 床が濡れていないか、アースされていない電源延長コードや保護アースの不備などがないかどうか、作業場所の安全を十分に確認してください。
- 回路の電源が切断されていると思い込まないで、*必ず*確認してください。
- 人身事故や装置障害を引き起こす可能性のある作業は行わないでください。
- 危険を伴う作業は、1 人では行わないでください。
- 電気事故が発生した場合は、次の手順に従ってください。
  - 十分注意して、自分自身が被害者にならないようにしてください。
  - アプライアンスの電源を切ってください。
  - 可能であれば、だれかに頼んで救護を呼んでもらいます。それができないときは、被害者の状態を判別してから助けを呼んでください。
  - 被害者が人工呼吸、心臓マッサージ、またはその他の治療を必要としているかどうか判断して、適切な処置を施してください。

さらに、電源は切断されているが、電話回線またはネットワーク ケーブルにはまだ接続されている機器を取り扱う場合は、次のガイドラインに従ってください。

- 雷が発生しているときには、電話線の接続を行わないでください。
- 防水設計されていない電話ジャックは、湿気の多い場所に取り付けないでください。
- 電話回線がネットワーク インターフェイスから切り離されていない限り、絶縁されていない電話ケーブルや端子には、触れないでください。
- 電話回線の設置または変更は、十分注意して行ってください。

静電破壊の防止

静電放電（ESD）によって機器が損傷し、電子回路に不具合が生じる可能性があります。静電放電は、電気プリント基板の取り扱いが不適切な場合に生じ、障害あるいは断続的障害を引き起こします。モジュールの取り外し時および交換時には、必ず ESD 保護手順に従ってください。

- 静電気に敏感な精密コンポーネントを開梱する場合は、アプライアンスへの設置の準備が整うまで静電気防止梱包材から取り出さないでください。静電気防止用の梱包材を取り外す直前に、必ず身体から静電気を放電してください。
- 精密コンポーネントを移動または輸送する際は、必ず静電気防止梱包を行います。
- 精密なコンポーネントは必ず耐静電気の安全な区域で処理します。可能な限り、静電気防止のフロアパッドや作業台パッドを使用します。
- CSACS-1121 シリーズ アプライアンスが電気的に接地されていることを確認してください。
- 静電気防止用リスト ストラップを肌に密着させて着用してください。クリップをアプライアンスの塗装されていない表面に止めて、不要な静電気がアースに流れるようにします。静電破壊と感電を防ぐために、リスト ストラップとコードは効果的に使用する必要があります。
- リスト ストラップがない場合は、アプライアンスの金属部分に触れて、身体から電気を逃がしてください。

注意：機器の安全を確保するために、静電気防止用リスト ストラップの抵抗値を定期的に検査してください。抵抗値は、1 ～ 10 Mohm でなければなりません。

持ち上げ時の注意事項

CSACS-1121 シリーズ アプライアンスは、アプライアンスに取り付けられているハードウェア オプションに応じて、15 ～ 33 ポンド（9.071 ～ 14.96 kg）の重さがあります。アプライアンスは、頻繁に移動されることを想定していません。アプライアンスを設置する前に、電源とネットワーク接続に対応するためにアプライアンスを後で移動する必要性が生じないように、設置場所が正しく準備されていることを確認してください。

アプライアンスまたは重い物を持ち上げる場合は、以下のガイドラインに従ってください。

- アプライアンスを持ち上げたり移動したりする前に、必ずすべての外部ケーブルを外してください。
- 足元を安定させ、両足で均等にシャーシの重量を支えるようにします。
- アプライアンスをゆっくり持ち上げます。突然移動したり、持ち上げるときに体をひねったりしないでください。
- 背中をまっすぐに保ち、背中ではなく脚で持ち上げます。アプライアンスを持ち上げるためにかがむ必要がある場合は、腰ではなく膝を曲げて、腰部の筋肉への負担を軽減してください。
- アプライアンスは下部から持ち上げてください。両方の手でアプライアンス外部の下側をつかみます。

設置場所の準備

CSACS-1121 シリーズ アプライアンスを設置する前に、次の点を準備することが重要です。

1. 設置場所を準備して（設置場所の計画（5 ページ）を参照）、設置計画または Method Of Procedure（MOP）を確認します。
2. アプライアンスを開梱して調べます。
3. アプライアンスを正しく設置するために必要な工具とテスト機器を収集します。

ここでは、次の項目について説明します。

- 設置場所の計画（5 ページ）
- 開梱と出荷内容の確認（9 ページ）
- 必要な工具と部品（11 ページ）
- インストレーション チェックリスト（12 ページ）
- サイト ログの作成（12 ページ）

設置場所の計画

警告：この装置は、立ち入りが制限された場所への設置を前提としています。立ち入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段を使用しないと入室できない場所を意味します。
ステートメント 1017

通常、設置場所を事前に準備しておく必要があります。準備の一環として、設置場所の平面図と、CSACS-1121 シリーズ アプライアンスを収容する機器ラックを入手します。

既存のアプライアンスの場所、および通信と電源を含む相互接続を判別します。通気の注意事項（通気に関するガイドライン（7 ページ）を参照）に従って、アプライアンスに十分な冷気を行きわたらせてください。

アプライアンスの設置に関与するすべての担当者（設置担当者、エンジニア、監督者）が、お客様による承認のために MOP の準備に参加する必要があります。詳細については、Method of Procedure（9 ページ）を参照してください。

次の項では、アプライアンスを設置する前に考慮する必要がある設置場所の要件に関するガイドラインについて説明します。

- ラックへの設置の安全に関するガイドライン（6 ページ）
- 設置場所の環境（7 ページ）
- 通気に関するガイドライン（7 ページ）
- 温度と湿度に関するガイドライン（8 ページ）
- 電源の考慮事項（8 ページ）
- Method of Procedure（9 ページ）

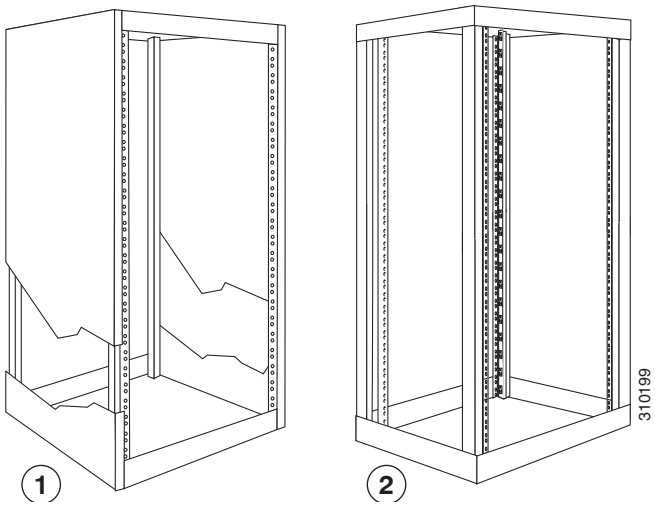
ラックへの設置の安全に関するガイドライン

CSACS-1121 シリーズ アプライアンスは、機器ラックに関する EIA 標準（EIA-310-D）に準拠する、ほとんどの 4 支柱（Telco タイプ）19 インチの機器ラックに設置できます。2 つの支柱にある取り付け穴の中心線間の距離は、18.31 インチ +/- 0.06 インチ（46.50 cm +/- 0.15 cm）でなければなりません。アプライアンスに付属のラック取り付けハードウェアは、ほとんどの 19 インチの装置ラックまたは Telco タイプのフレームに適しています。

注: 可能な限り 4 支柱ラックを使用することが強く推奨されます。またラックには、アプライアンスを取り付けるためにマウント フランジ付きの支柱が少なくとも 2 つ*必要です*。

図 1（6 ページ）に、4 支柱装置ラックの一般的な 2 つの例を示します。

図 1　4 支柱装置ラックのタイプ



4 支柱（部分閉鎖型）ラック

図 1（6 ページ）の図 1 に、前面に 2 つの支柱があり、背面にさらに 2 つの支柱がある、自立型の部分的に密閉されたラックを示します。CSACS-1121 シリーズ アプライアンスは、このような閉鎖型ラックに設置できます。これは、このアプライアンスでは、内部コンポーネントの許容動作温度を保持するために、冷気が妨げられずにシャーシの前面に流れ、背面から出て行くようにする必要があるためです。

4 支柱（オープン）ラック

図 1（6 ページ）の図 2 に、前面に 2 つの支柱があり、背面に 2 つの支柱がある、自立型の 4 支柱のオープン ラックを示します。このタイプのラックの支柱は、多くの場合調整可能であるため、ラックの前面と面一に取り付けるのではなく、ラックの奥にラック取り付け型の装置を配置できます。

ラックに CSACS-1121 シリーズ アプライアンスを設置する前に、次の推奨事項を確認してください。

- ラックにアプライアンスを設置するには、2 人以上必要です。
- 室温が 35 °C（95 °F）を下回っていることを確認します。
- 通気孔をふさがないでください。通常、6 インチ（15 cm）のスペースで通気が行きわたります。
- アプライアンスの設置の際は、ラックの一番下から始めるように計画してください。
- 複数のアプライアンスをラックの外側に同時に延ばさないでください。
- アプライアンスは、正しく接地されたコンセントに接続してください。
- ラックに複数のデバイスを設置する場合は、電源コンセントの過負荷が発生しないようにしてください。
- 50 kg（110 ポンド）を超える重さの物をラック取り付け型デバイスの上部に置かないでください。

設置場所の環境

正常に動作させるには、アプライアンスの配置、装置ラックまたは配線室のレイアウトが非常に重要です。複数の装置を近づけて設置したり、換気が不十分であったり、手の届かないパネルがあったりすると、誤操作やシャットダウンの原因となり、メンテナンスが困難になります。アプライアンスの前面パネルおよび背面パネルへのアクセスについて計画を立てます。

次の注意事項は、アプライアンスの動作環境を適切にし、環境条件による装置の障害を防止するのに役立ちます。

- アプライアンスが動作する部屋の空気循環が十分であることを確認します。電子機器は放熱します。十分に空気循環されていないと、室内の温度が高くなり、機器を許容動作温度に冷却できなくなる場合があります。詳細については、通気に関するガイドライン（7 ページ）を参照してください。
- ラックの設置場所に、AC 電源コンセント、アース、およびネットワーク ケーブルの設備があることを確認してください。
- 十分なスペースを確保して、設置中にラックの周囲で作業できるようにします。用意するもの：
  - アプライアンスの移動、位置合わせ、挿入のために、ラックに隣接して少なくとも 3 フィート（9.14 m）。
  - 設置後のメンテナンスのために、アプライアンスの前面と背面に少なくとも 24 インチ（61 cm）の空間。
- 2 つの支柱またはレールの間にアプライアンスを取り付けるには、使用可能な開口（2 つのマウント フランジの*内*端間の幅）は少なくとも 17.7 インチ（45.0 cm）でなければなりません。

  注：ラックマウント キットには 2 支柱ラックは入っていません。
- 適切な方法でケーブルの張力をゆるめ、ケーブルと機器の接続を保護します。
- ネットワーク インターフェイス ケーブルへのノイズ干渉を防止するために、ケーブルが電源コードと直交または平行にならないように配線します。
- 機器の破損を防ぐため、静電破壊の防止（4 ページ）に記載されている静電放電の防止手順に必ず従ってください。静電放電による損傷によって、即時または断続的な機器障害が発生する可能性があります。

通気に関するガイドライン

機器ラック内で十分な通気を確保するには、ラックの前面と背面に少なくとも 6 インチ（15.24 cm）の空間を維持することを推奨します。機器ラックと、ラックに配置されているアプライアンス内の通気がブロックまたは制限されている場合、またはラックに流れる換気の温度が高すぎると、ラックと、ラックに配置されているアプライアンス内で適正温度を超えた状態が発生する可能性があります。

また、設置場所では、可能な限り埃のない状態にする必要があります。アプライアンスのファンには埃が詰まりやすく、機器ラックと、ラックに配置されているアプライアンス内で冷気の流れが低下します。この低下によって、適正温度を超えた状態が発生するリスクが高まります。

さらに、次のガイドラインは、装置ラックの構成を計画する場合に役立ちます。

- 通気の他に、ラックの周囲に、メンテナンスに必要な空間を確保する必要があります。
- オープンラックにアプライアンスを設置する場合、ラックのフレームで前面の吸気口や背面の排気口をふさがないように注意してください。

温度と湿度に関するガイドライン

表 1（8 ページ）に、CSACS-1121 シリーズ アプライアンスの稼働環境の設置場所と非稼働環境の設置場所の要件をリストします。アプライアンスは通常、一覧に記載された範囲内で稼働します。ただし、温度の測定値が最小または最大パラメータに近づいている場合、潜在的な問題があることを示します。

アプライアンスを取り付ける前に設置場所のプランニングと準備を適切に行うことで、クリティカルな値に近づく前に環境の異常を予測して修正し、正常な動作を維持してください。

表 1　稼働環境と非稼働環境の仕様

仕様	最小ハードウェア	最大数
動作時温度	10°C（50°F）	35°C（95°F）
非動作時および保管時の温度	-40 °F（°C）	70°C（158°F）
動作時の湿度（結露しないこと）	10%	90%
非動作時および保管時の湿度（結露しないこと）	5%	95 %
動作時の振動	5 ～ 500 Hz、2.20 g RMS ランダム	–

電源の考慮事項

CSACS-1121 シリーズ アプライアンスは、AC 入力の電源だけで構成する必要があります。すべての電源接続が National Electrical Code（NEC）の規則と規制、および地域の規定に準拠していることを確認します。アプライアンスへの電源接続を計画する際には、次の注意事項と推奨事項に従う必要があります。

- 設置前に設置場所の電源を確認し、設置後も定期的に確認して、クリーンな（スパイクやノイズのない）電力が供給されるようにしてください。必要に応じて、電力調整器を取り付けてください。
- AC 電源には次の機能があります。
  - 110 V または 220 V 運用の自動選択機能。
  - すべてのアプライアンスの電気コード（電源コードの近くにあるラベルは、アプライアンスの正しい電圧、周波数、電流引き込み、および消費電力を示しています）。

警告：この製品は、設置する建物に短絡（過電流）保護機構が備わっていることを前提に設計されています。120 VAC、15 A 以下（米国の場合。その他の国では 240 VAC、10 A）のヒューズまたは回路ブレーカーが、位相導体（すべての通電導体）で使用されていることを確認してください。ステートメント 13

- 装置ラックで適切に接地し、雷や電力サージによる損傷を防止してください。

警告：この装置は必ずアース接続を行う必要があります。絶対にアース導体を破損させたり、アース線が正しく取り付けられていない装置を稼働させたりしないでください。アースが適切かどうかがはっきりしない場合には、電気検査機関または電気技術者に確認してください。ステートメント 1024

- オペレータによる調整の必要がない、100 ～ 240 の VRMS と 50/60 Hz の範囲内の入力電圧と周波数で稼働する AC 入力電源モジュール。表 2（9 ページ）に、電気入力に関する追加情報を示します。

表 2　電気入力の仕様

仕様	最小ハードウェア	最大数
正弦波入力	50 Hz	60 Hz
入力電圧の低範囲	100 V ac	127 V ac
入力電圧の高範囲	200 V ac	240 V ac
概算入力キロボルト アンペア（kVA）	0.102 kVA	0.55 kVA

Method of Procedure

以前に説明したように、準備には設置計画または MOP の確認が含まれます。MOP（設置前の作業のチェックリストと、設置に進む前に対処して同意する必要がある考慮事項）の例は次のとおりです。

1. 担当者を割り当てます。
2. 担当者、機器、および工具の保護要件を決定します。
3. 保守に影響する可能性がある事故を評価します。
4. 設置の時期をスケジュールします。
5. スペースの要件を決定します。
6. 所要電力を決定します。
7. 必要な手順またはテストを特定します。
8. 機器の計画時に、設置を計画している各 CSACS-1121 シリーズ アプライアンスを配置する暫定的な決定を行います。
9. このハードウェア インストレーション ガイドを確認します。
10. 設置のために交換可能なパーツ（ネジ、ボルト、ワッシャなど）のリストを確認して、特定します。
11. 必要な工具とテスト機器が使用可能であることを確認するために、必要な工具リストを調べます。詳細については、必要な工具と部品（11 ページ）を参照してください。
12. 設置を実行します。

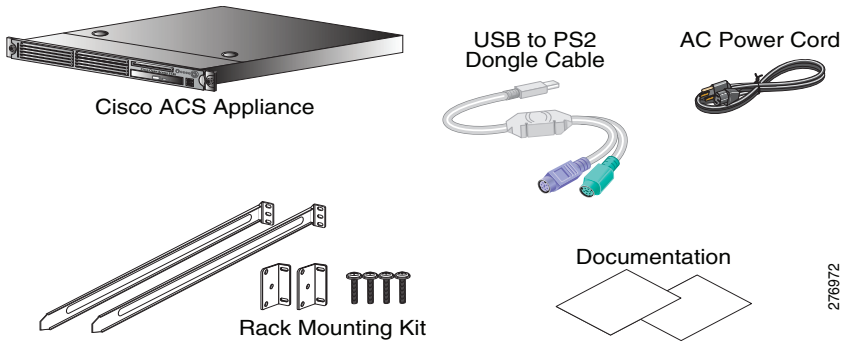
開梱と出荷内容の確認

CSACS-1121 シリーズ アプライアンスの出荷パッケージは、出荷中の通常の運搬に関連する製品損傷の可能性を減らすように設計されています。製品の損傷の可能性を減らすには、アプライアンスをシスコの本来の梱包材で移送してください。そうしない場合、アプライアンスが損傷を受ける可能性があります。また、設置の準備ができるまでは、アプライアンスを輸送用の箱から取り出さないでください。

アプライアンス、ケーブル、および注文したオプションの機器は、複数の箱で出荷されることがあります。損傷を受けたり、足りなかったりする項目を記録するために、*Notes* セクションがあります。図 2（10 ページ） に、CSACS-1121 シリーズ アプライアンスでの出荷項目を表示します。

注：CSACS-1121 シリーズ アプライアンスの梱包材は廃棄しないでください。アプライアンスを移動または出荷する場合に、将来梱包材料が必要になります。

図 2　CSACS-1121 シリーズ アプライアンスと一緒に出荷される品目



出荷時の損傷がないかどうか、すべての品目を調べます。損傷を受けている物がある場合、またはアプライアンスの設置または構成の問題が発生した場合は、カスタマー サービス担当者にお問い合わせください。

注: ラックマウント キットには 2 支柱ラックは入っていません。

『Cisco Information Packet』と保証

『*Cisco Information Packet*』には、保証、保守、およびサポート情報が記載されています。

次の手順を実行して、Cisco.com から『*Cisco Information Packet*』、保証、およびライセンス契約書にアクセスし、これらをダウンロードしてください。

インターネット ブラウザを起動し、次のサイトにアクセスします。

http://www.cisco.com/en/US/products/prod_warranties_listing.html

[Warranties and License Agreements] ページが表示されます。

『*Cisco Information Packet*』を参照するには、次の手順を実行します。

1. [Information Packet Number] フィールドをクリックし、製品番号 78-5235-03D0 が強調表示されていることを確認します。
2. 文書を表示する言語を選択します。
3. [Go] をクリックします。

   情報パケットの [Cisco Limited Warranty and Software License] ページが表示されます。
4. このページから文書をオンラインで見ることも、[PDF] アイコンをクリックして、文書をダウンロードし、印刷することもできます。

   PDF ファイルの表示と印刷には Adobe Acrobat Reader が必要です。Adobe の Web サイトからダウンロードできます。

お手持ちの製品について、翻訳またはローカライズされた保証情報を表示するには、次の手順を実行します。

1. [Warranty Document Number]フィールドに、次の製品番号を入力します。

   78-5236-01C0
2. 文書を表示する言語を選択します。
3. [Go] をクリックします。

   Cisco warranty ページが表示されます。

4. このページから文書をオンラインで見ることも、PDF アイコンをクリックして、文書を PDF 形式でダウンロードし、印刷することもできます。

また、Cisco Service and Support の Web サイトにアクセスして、サポートを受けることもできます。

http://www.cisco.com/en/US/support/

ハードウェア保証期間

90 日間

ハードウェアに関する交換、修理、払い戻しのポリシー

シスコ、またはその代理店では、返品許可（RMA）要求を受領してから 10 営業日以内に交換部品を出荷するように商業上合理的な努力を払います。実際の配達所要日数は、お届け先によって異なります。

シスコは購入代金を払い戻すことにより一切の保証責任とさせて頂く権利を留保します。

返品許可（RMA）番号の入手

製品を購入されたシスコの代理店にお問い合わせください。製品を直接シスコから購入された場合は、シスコの営業担当者にお問い合わせください。

次の項目を記入し、参照用に保管してください。

製品の購入先	—
購入先の電話番号と Web サイトのロケーション	—
製品モデル番号	—
製品シリアル番号[1]	—
保守契約番号	—

1. 詳細については、製品シリアル番号の場所（2 ページ）および 製品シリアル番号の場所（7 ページ）を参照してください。

必要な工具と部品

注意：ラックマウント キットのネジ袋にはラック用のネジが 8 本入っています。これらのネジを調べて、ラックの穴に合った適切なサイズであることを確認する必要があります。ラックのネジ穴に誤ったサイズのネジを使用すると、ラックが損傷を受ける可能性があります。

4 支柱ラックに CSACS-1121 シリーズ アプライアンスを設置するために必要な工具および機器は、次のとおりです。

警告：この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。
ステートメント 1030

- 静電気防止用コードとリスト ストラップ。
- No.2 プラス ドライバ。
- メモリまたはその他のコンポーネントをアップグレードする場合は、カバーを取り外すためにマイナス ドライバ（小型の 3/16 インチ（0.476 cm）と中型の 1/4 インチ（0.625 cm））。
- ラックマウントキット。キットの内容の詳細については、4 支柱ラックマウント ハードウェア キット（2 ページ）を参照してください。

- LAN ポートに接続するためのケーブル（構成によって異なる）。
- イーサネット（LAN）ポートへの接続用にイーサネット スイッチ。

CSACS-1121 シリーズ アプライアンスの初期構成を行うには、次のいずれかが必要です。

- USB キーボードとビデオ グラフィック アレイ（VGA）モニタ。

  または

- 9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、およびハードウェア フロー制御なし用に構成されたコンソール端末（ASCII 端末または端末エミュレーション ソフトウェアが実行されている PC）。
- シリアル（コンソール）ポートに接続するためのコンソール ケーブル。ヌルモデム ケーブルが推奨されます。

インストレーション チェックリスト

設置を支援し、行った作業の履歴レコードを提供するには、次のインストレーション チェックリストを使用してください。このチェックリストのコピーを作成し、各タスクの完了時にエントリにマークを付けます。

チェックリストに入力したら、CSACS-1121 シリーズ アプライアンスごとにチェックリストのコピーを、新規アプライアンスの他のレコードとともに設置場所のログ（設置場所のログの作成については、サイト ログの作成（12 ページ）を参照）に含めます。

設置場所のインストレーション チェックリスト：CSACS-1121：		
タスク	確認者	日付（Date）
インストレーション チェックリストをコピーする	—	—
サイト ログに背景説明を含める	—	—
設置場所の電源電圧を確認する	—	—
設置場所の電源チェック完了	—	—
必要な工具が使用可能であることを確認する	—	—
追加の機器が使用可能であることを確認する	—	—
CSACS-1121 シリーズ アプライアンスを受け取る	—	—
資料『*Cisco Information Packet*』を受け取る	—	—
アプライアンス コンポーネントを確認する	—	—
最初の電源投入成功	—	—
ASCII 端末（ローカル設定用）を確認する	—	—
信号の距離制限を確認する	—	—
起動シーケンス手順完了	—	—
初期動作を確認する	—	—

サイト ログの作成

設置場所のログ（設置場所のログのサンプルについては、サイト ログを参照してください）は、CSACS-1121 シリーズ アプライアンスの設置と保守に関連するすべてのアクションのレコードを提供します。作業者全員がすぐに参照できるように、サイト ログはアプライアンスのそばに保管してください。

インストレーション チェックリスト（インストレーション チェックリスト（12 ページ）を参照）を使用して、アプライアンスの設置とメンテナンスの手順を確認します。サイト ログ エントリには、次の項目が含まれていることがあります。

- 設置の進行：アプライアンスのインストレーション チェックリストのコピーを作成して、サイト ログに挿入します。各タスクの完了時に、エントリを作成します。
- アップグレード、取り外し、およびメンテナンス手順：進行中のアプライアンスのメンテナンスと拡張履歴のレコードとして、サイト ログを使用します。アプライアンスでタスクを実行するたびに、サイト ログを更新して、次の情報を反映させます。
  - 新規アダプタ カードの取り付け
  - アダプタ カードの取り外しまたは交換と、その他のアップグレード
  - 設定変更
  - 保守のスケジュールと要件
  - 実行した保守手順
  - 間欠的な問題
  - コメントとメモ

イーサネットとコンソール ポートに関する考慮事項

ACS 5.8.1 は複数のネットワーク インターフェイス コネクタをサポートしています。CSACS-1121 シリーズ アプライアンスの背面パネルには、4 個のイーサネット コネクタがあります。複数のネットワーク インターフェイス コネクタの詳細については、複数のネットワーク インターフェイス コネクタ（9 ページ）を参照してください。GigabitEthernet ポートには UTP ケーブルを使用します。シスコでは、カテゴリ 5 UTP ケーブルを推奨します。セグメントの最大距離は 328 フィート（100 m）です。UTP ケーブルは、通常の電話に使用されるケーブルと似ています。ただし、UTP ケーブルは、電話ケーブルでは満たされない特定の電気規格を満たします。ケーブルは含まれていません。

アプライアンスには、（コンソール端末を使用して）アプライアンスにローカルでアクセスできるようにする非同期シリアル コンソール ポートが含まれています。ここでは、コンソール端末（ASCII 端末または端末エミュレーション ソフトウェアが実行されている PC のいずれか）をコンソール ポートに接続する前に考慮すべき重要なケーブル接続情報について説明します。

注：コンソール ケーブルは CSACS-1121 シリーズ アプライアンスに含まれていません。

イーサネットとコンソール ポートに関する考慮事項

Cisco 1121 Secure Access Control System ハードウェアの設置

この章では、CSACS-1121 シリーズ アプライアンスを設置しネットワークに接続する方法について説明します。

内容は、次のとおりです。

- ラックマウント構成のガイドライン（1 ページ）
- CSACS-1121 シリーズ アプライアンスの 4 支柱ラックへのマウント（2 ページ）
- ケーブルの接続（7 ページ）
- CSACS-1121 シリーズ アプライアンスの電源投入（17 ページ）
- ラック キャビネットの輸送の準備（19 ページ）
- CSACS-1121 シリーズ アプライアンスの取り外しまたは交換（20 ページ）

設置を始める前に、『*Regulatory Compliance and Safety Information for the Cisco 1121 Secure Access Control System*』を参照してください。

警告：この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。ステートメント 1030

警告：この装置は、立ち入りが制限された場所への設置を前提としています。立ち入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段を使用しないと入室できない場所を意味します。
ステートメント 1017

ラックマウント構成のガイドライン

各 CSACS-1121 シリーズ アプライアンスには、ラック ハンドル（工場にて取り付け）が備わっています。アプライアンスを 4 支柱ラックに設置する際にはこのハンドルを使用します。4 支柱ラック仕様（内側の幅は 17.5 インチ（44.45 cm）であることが必要です）に準拠した 19 インチ（48.3 cm）装置ラックに、アプライアンスをフロント（フラッシュ）マウントまたはミッドマウントできます。

アプライアンスはブラケットにマウントします。アプライアンスをラックに設置する際には、マウントのために 1 つ分の EIA 1.75 インチ（4.4 cm）垂直マウント スペースまたは 1 ラック ユニット（RU）が必要です。

注意：冷却用の空気が前面から取り込まれ、アプライアンス内を循環してアプライアンスの背面から排出されるように、CSACS-1121 シリーズ アプライアンスの前後に空間を確保する必要があります。

ラックへの設置の安全に関するガイドライン（6 ページ）および次の情報は、装置ラックの構成を計画するために役立ちます。

- アプライアンスを装置ラックにマウントする際には、必ずラックを床にボルトで固定してください。
- ラックには複数のアプライアンスを設置できますが、設置された全アプライアンスの重さでラックが不安定にならないようにしてください。

注意：ラック内装置の重量を考慮して、一部の装置ラックでは、天井のブラケットにも固定するようになっています。このタイプの設置を行う場合は、アプライアンスを設置するために使用するラックは必ず建物の躯体に固定してください。

- 通気に関するガイドライン（7 ページ）で説明したように、空気が適切に吸入および排出されるように、アプライアンスの前後に 6 インチ（15.2 cm）の間隔を確保してください。
- アプライアンスを過密状態のラックに設置しないでください。ラック内の他のアプライアンスとの間での空気の流れにより、アプライアンスを通過する正常な冷却空気の流れが妨げられ、アプライアンスの内部が過熱状態になる可能性が高まります。
- アプライアンスの保守のために、ラックの前後に 24 インチ（61 cm）以上の空間を確保してください。

注意：アプライアンスが過熱状態にならないようにするため、密閉型ラックや、適切な換気または空気調整のなされていない部屋にはアプライアンスを設置しないでください。

- ケーブル管理については、各地の習慣に従ってください。アプライアンスに接続されたケーブルが、装置の保守やアップグレードを行うためのアクセスの妨げにならないようにしてください。

  注：ラックマウント ハードウェア キットに 2 支柱装置ラックは含まれていません。

CSACS-1121 シリーズ アプライアンスの 4 支柱ラックへのマウント

警告：ラックに設置したアプライアンスがスライドレール全幅に広がる場合、不安定になるため転倒に注意してください。重大なケガにつながる恐れがあります。レールを伸ばした場合や地震が発生した場合でもラックが不安定にならないようにするため、ラックを床に固定してください。

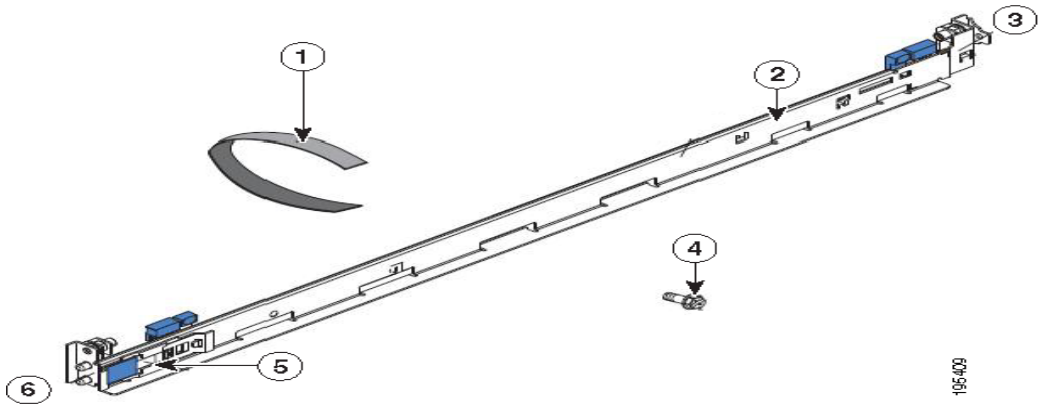
ここでは、次の項目について説明します。

- 4 支柱ラックマウント ハードウェア キット（2 ページ）
- スライド レールのラックへの取り付け（3 ページ）
- アプライアンスのスライド レールへの取り付け（5 ページ）

4 支柱ラックマウント ハードウェア キット

図 1（2 ページ）に、CSACS-1121 シリーズ アプライアンスを 4 支柱ラックに設置するのに必要な部品を示します。

図 1　スライド レール ハードウェア上のリリース レバー



次の表で、図 1（2 ページ）の各コンポーネントについて説明します。

1	ケーブル ストラップ	4	M6 ネジ
2	スライド レール	5	輸送用ブラケット
3	レールの前面	6	レールの背面

表 1(3 ページ) に、ラックマウント ハードウェア キット(シスコ製品番号 CSACS-1U-RAILS)の内容を示します。

表 1　ラックマウント ハードウェア キット

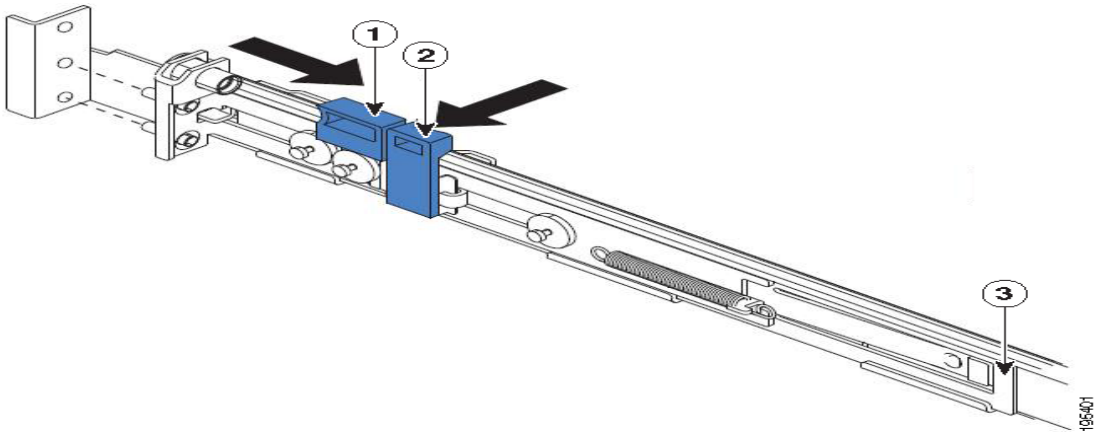
項目	数量
スライド レール	2
ケーブル ストラップ	6
M6 ネジ	6

スライド レールのラックへの取り付け

CSACS-1121 シリーズ アプライアンスをラックに取り付けるには、次の手順を実行します。

1. スライド レールの背面にあるレール調整ブラケット(図 2(3 ページ) を参照)を押して、ブラケットが動かないようにします。
2. 調整タブ 1 と 2(図 2(3 ページ) を参照)を押し、レールロック キャリアを、カチッとはまるまでスライド レールの前面に向けてスライドさせます。
3. 調整タブ 1 と 2 を押し、レールロック キャリアを、カチッとはまるまでスライド レールの背面に向けてスライドさせます。

図 2　スライド レールのラックへの取り付け



次の表で、図 2(3 ページ) の各コンポーネントについて説明します。

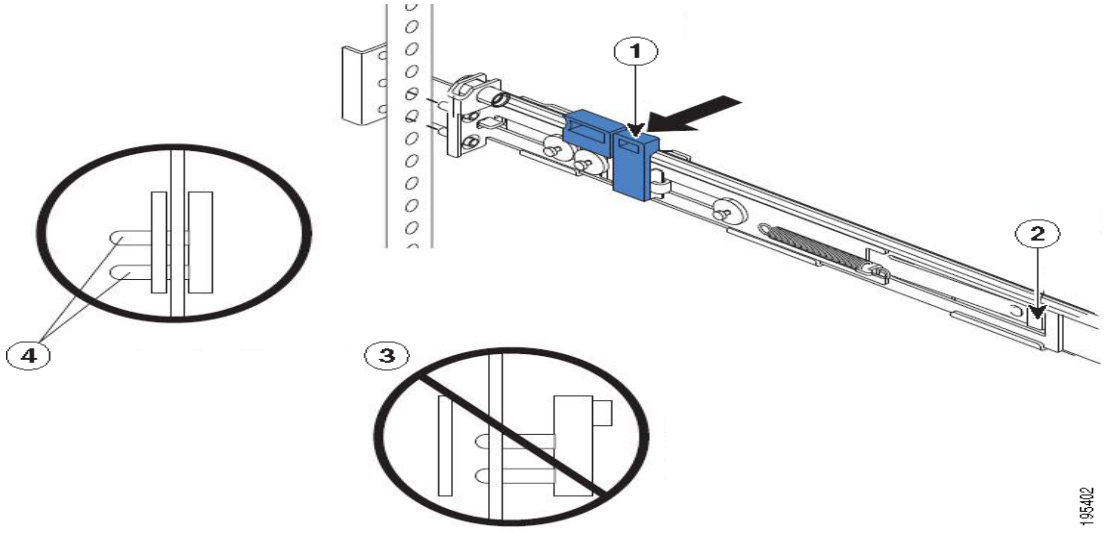
1	調整タブ 1	3	レール調整ブラケット
2	調整タブ 2		

スライドレールの長さを調整する必要がある場合は、リリース タブ(図 3(4 ページ) を参照)を持ち上げ、カチッとはまるまでスライド レールの背面からレール調整ブラケットを完全に伸ばします。

4. 背面レールロック キャリアのピンを、後面マウント フランジの穴に合わせます。
5. 調整タブ(図 3(4 ページ) を参照)を押して、スライド レールの背面を背面マウント フランジに固定します。

注:ピンは、マウント フランジとスライド レールに完全に差し込んでください。

図 3　スライドレールの長さの調整



次の表で、図 3（4 ページ）の各コンポーネントについて説明します。

1	調整タブ	3	ピンがマウント フランジとスライド レールに完全に差し込まれていない
2	リリース タブ	4	ピンがマウント フランジとスライド レールに完全に差し込まれている

6. 前面レールロック キャリア上のピン（図 4（5 ページ）を参照）を、前面マウント フランジに合わせます。

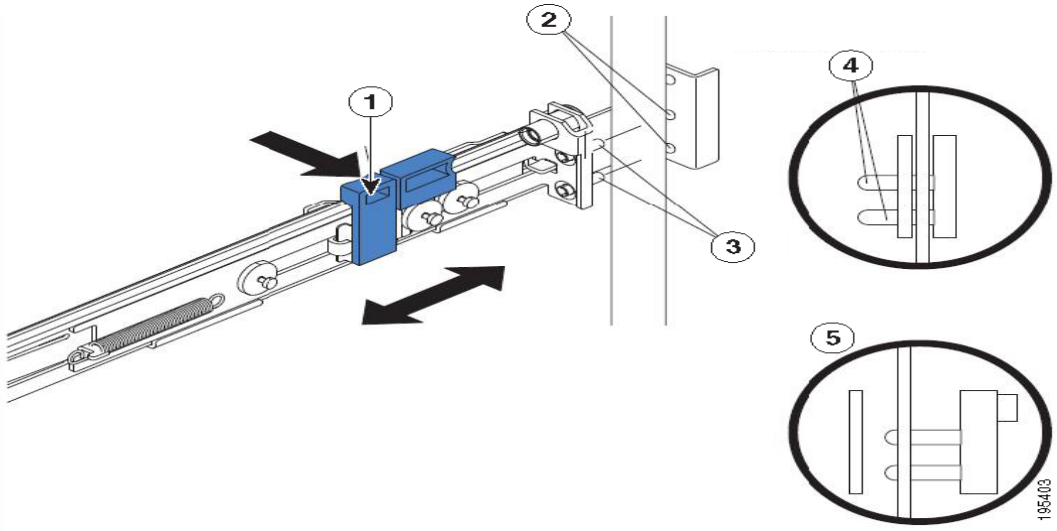
   レール長を調整した場合は、レールロック キャリアをスライド レールの背面に向けて押し、スライド レールをマウント フランジに合わせます。

7. 調整タブを押して、スライド レールの前面を前面マウント フランジに固定します。

   注：ピンは、マウント フランジとスライド レールに完全に差し込んでください。

8. もう 1 つのスライド レールに対してこれらのステップを繰り返します。

図 4　スライド レールとマウント フランジの位置合わせ



次の表で、図 4（5 ページ）の各コンポーネントについて説明します。

1	調整タブ	4	ピンがマウント フランジとスライド レールに完全に差し込まれている
2	マウント フランジ	5	ピンがマウント フランジとスライド レールに完全に差し込まれていない
3	ピン		

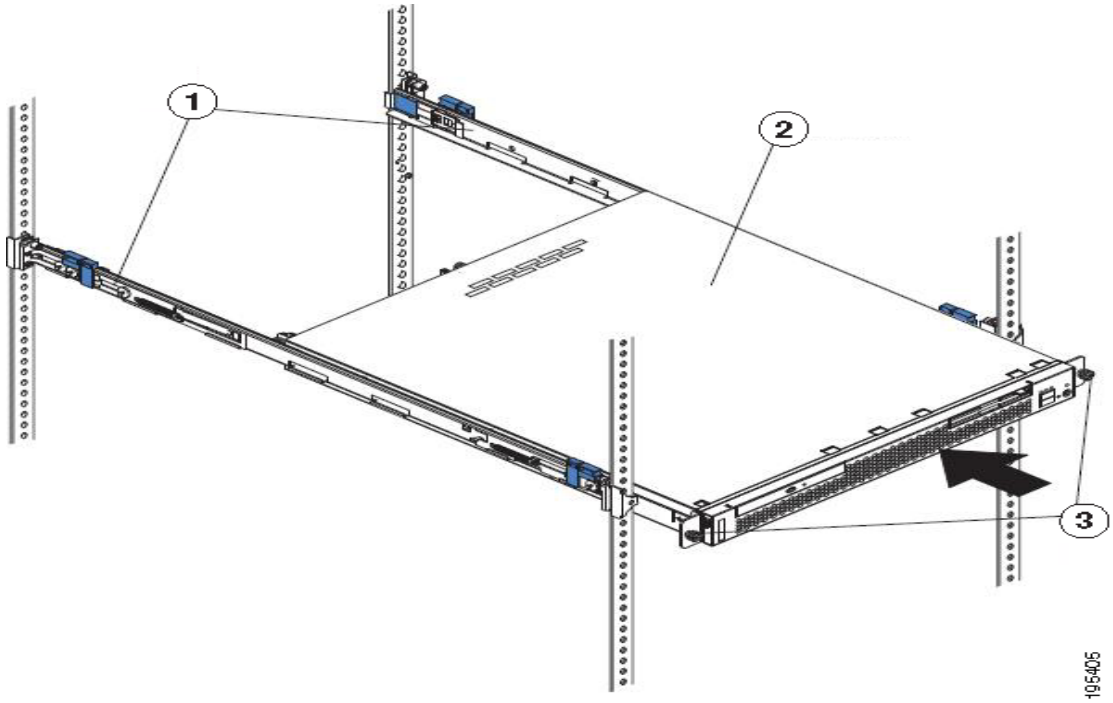
アプライアンスのスライド レールへの取り付け

CSACS-1121 シリーズ アプライアンスをスライド レールに取り付けるには、次の手順を実行します。

1. サーバをスライド レールに合わせ、ラック キャビネットに完全に収まるまで押します。
2. 取り付けネジで、サーバを前面マウント フランジに固定します（図 5（6 ページ）を参照）。

   注：サーバがラックのキャビネットに挿入される際の妨げとなる場合を除き、輸送用ブラケットはスライドレールに付けたままにします。輸送用ブラケットを取り外すときは、手順 3 を参照してください。

図 5　スライド レール上でのサーバの位置合わせ



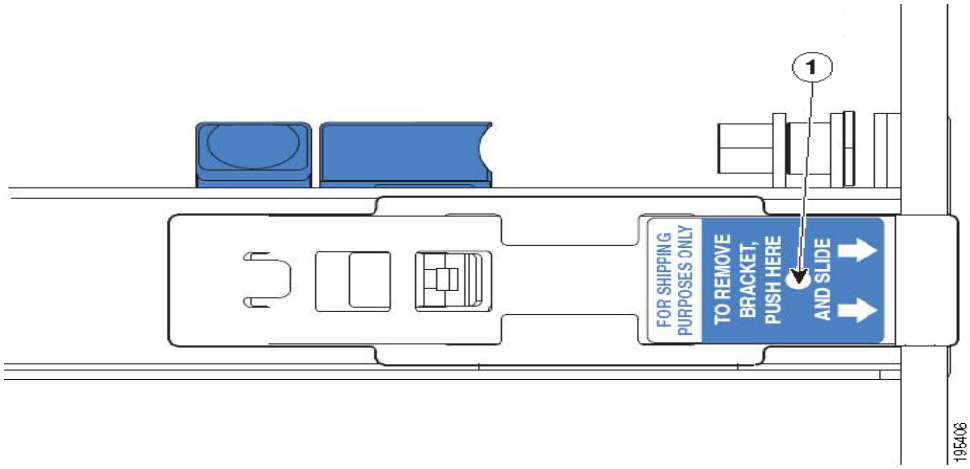
次の表で、図 5（6 ページ）の各コンポーネントについて説明します。

1	輸送用ブラケット	3	取り付けネジ
2	ACS サーバ		

3. 輸送用ブラケット上で、図のようにリリース タブ（図 6（7 ページ）を参照）を押し、スライド レールから輸送用ブラケットを取り外します。
4. もう 1 つの輸送用ブラケットにも手順 3 を繰り返します。取り外したブラケットは、将来使用する場合に備えて保管しておきます。

注: サーバが取り付けられた状態でラック キャビネットを輸送する場合は、その前に輸送用ブラケットをスライド レールに再度取り付ける必要があります。輸送用ブラケットを再度取り付けるには、逆の手順を実行します。

図 6　輸送用ブラケットの取り外し



次の表で、図 6（7 ページ）のコンポーネントについて説明します。

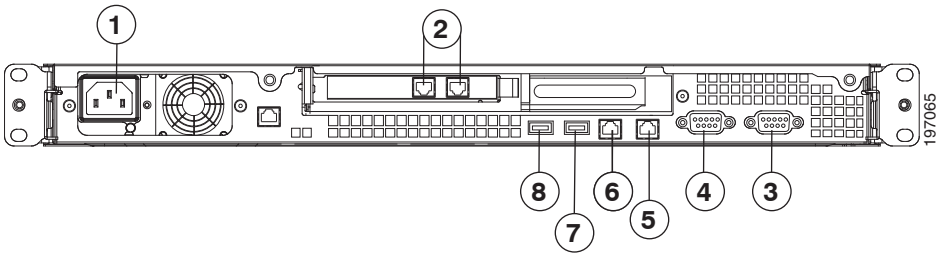
1	リリース タブ		

ケーブルの接続

ここでは、CSACS-1121 シリーズ アプライアンスをネットワークおよびアプライアンス コンソールに接続する方法について説明します。この項では、次の内容について説明します。

- ネットワーク インターフェイスの接続（8 ページ）
- コンソールの接続（16 ページ）
- キーボードとビデオ モニタの接続（17 ページ）
- ケーブル管理（17 ページ）

図 7　CSACS-1121 シリーズ アプライアンスの背面図

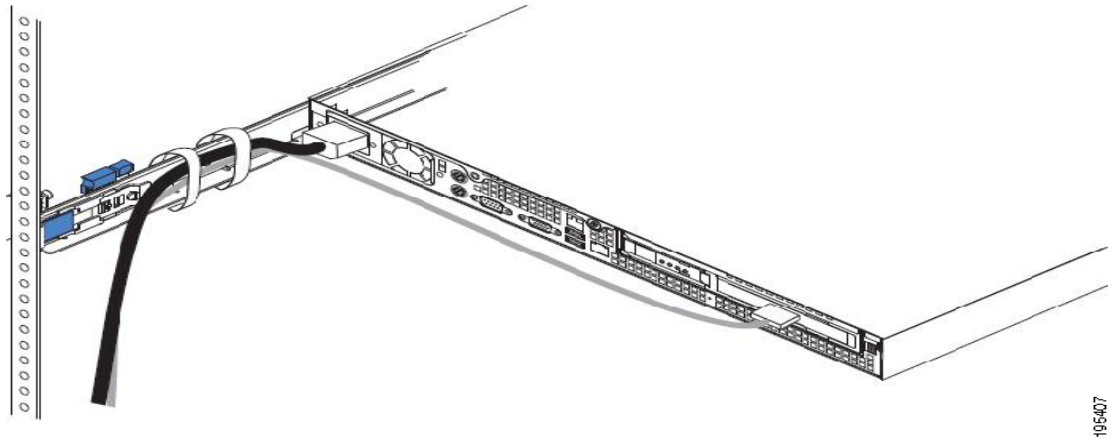


次の表で、図 7（7 ページ）の各コンポーネントについて説明します。

1	AC 電源コンセント	5	（ブロック）GigabitEthernet 1
2	（ブロック）GigabitEthernet	6	（使用中）GigabitEthernet 0
3	シリアル コネクタ	7	USB 3 コネクタ
4	ビデオ コネクタ	8	USB 4 コネクタ

ケーブル（必要に応じてキーボード、モニタ ケーブルなど）をサーバの背面に接続します。ケーブルはサーバの左隅にまとめ（背面から見たときに図 8（8 ページ）のようにします）、ケーブル ストラップを使用してスライド レールに固定します。

図 8　ケーブルの接続



ネットワーク インターフェイスの接続

警告：雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

ここでは、CSACS-1121 シリーズ アプライアンス イーサネット ポートを接続する方法について説明します。

イーサネット コネクタは、Serial over LAN（SoL）ケーブルをサポートしています。RJ-45 ポートは、標準的なストレートおよびクロス カテゴリ 5 Unshielded Twisted-Pair（UTP）ケーブルをサポートしています。シスコではカテゴリ 5 UTP ケーブルを販売していません。市販のケーブルを使用してください。

ケーブルをアプライアンスのイーサネット ポートに接続するには、次の手順を実行します。

1. アプライアンスの電源がオフになっていることを確認します。
2. ケーブルの一方の端を、アプライアンス上の GigabitEthernet 0 ポートに接続します。
3. 他方の端をネットワークのスイッチに接続します。

イーサネット ポート コネクタ

CSACS 1121 シリーズ アプライアンスには、2 つの統合型デュアル ポート イーサネット コントローラが搭載されています。SNS-3400 シリーズ アプライアンスには、4 つの統合型デュアル ポート イーサネット コントローラが搭載されています。ACS は複数の NIC をサポートしています。詳細については、複数のネットワーク インターフェイス コネクタ（9 ページ）を参照してください。これらのコントローラでは 10-Mb/s、100-Mb/s、または 1000-Mb/s ネットワークに接続するためのインターフェイスと全二重（FDX）機能が提供され、イーサネット LAN 上でデータを同時に送受信できます。

イーサネット ポートにアクセスするには、カテゴリ 3、4、5、5E、または 6 のシールドなしツイストペア（UTP）ケーブルを、アプライアンスの背面にある RJ-45 コネクタに接続します。

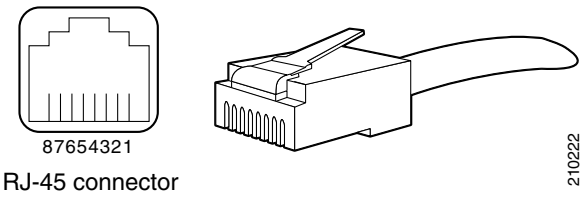
表 2（9 ページ）に、UTP ケーブルのカテゴリを示します。

表 2　イーサネット ケーブル接続ガイドライン

タイプ	説明
10BASE-T	EIA カテゴリ 3、4、または 5 UTP（2 または 4 ペア）、最大 328 フィート（100 m）
100BASE-TX	EIA カテゴリ 5 UTP（2 ペア）、最大 328 フィート（100 m）
1000BASE-T	EIA カテゴリ 6 UTP（推奨）、カテゴリ 5E UTP または 5 UTP2 ペア）、最大 328 フィート（100 m）

図 9（9 ページ） に、イーサネット RJ-45 ポートとプラグを示します。

図 9　RJ-45 ポートとプラグ



RJ-45 connector

表 3（9 ページ） の一覧では、コネクタで使用される RJ-45 ピン信号について説明します。

表 3　イーサネット ポートのピン配列

イーサネット ポートのピン	信号	説明
1	TxD+	送信データ +
2	TxD-	送信データ -
3	RxD+	受信データ +
4	終端ネットワーク	接続なし
5	終端ネットワーク	接続なし
6	RxD-	受信データ -
7	終端ネットワーク	接続なし
8	終端ネットワーク	接続なし

複数のネットワーク インターフェイス コネクタ

Cisco SNS3500 や Cisco SNS3400、仮想マシン、または CSACS-1121 プラットフォームと ACS 5.8.1 の組み合わせでは、イーサネット 0、イーサネット 1、イーサネット 2、イーサネット 3、イーサネット 4、イーサネット 5 の 6 種類のネットワーク インターフェイスが使用できます。

注: システム障害を防ぐため、イーサネット インターフェイス 0 がオンになっており、正常に動作していることを確認します。

表 4（10 ページ） に、ネットワーク インターフェイス間に分散された ACS 5.8.1 サービスを示します。

表 4　ネットワーク インターフェイス間での機能インターフェイスの分布

機能インターフェイス	ネットワーク インターフェイス
顧客ロギング	イーサネット 0 のポート
デバイス管理（TACACS+）	すべて
分散管理	イーサネット 0 のポート
外部 ID ストア（AD、LDAP、および RSA）	イーサネット 0 のポート
管理 GUI（HTTP）	イーサネット 0 のポート
管理 CLI（Secure Shell（SSH））	イーサネット 0 のポート
モニタリングとトラブルシューティング/ACS View の syslog	すべて
ネットワーク アクセス（RADIUS）	すべて
RADIUS プロキシ	すべて
TACACS+ プロキシ	すべて

ACS の管理機能ではイーサネット インターフェイス 0 だけが使用されますが、認証、許可、およびアカウンティング（AAA）プロトコルでは、設定されているすべてのネットワーク インターフェイスが使用されます。分散導入では、ACS ノードをイーサネット 0 だけに接続する必要があります。syslog メッセージは、ログ コレクタのイーサネット 0 インターフェイスで送受信されます。潜在的なセキュリティ上の問題を防止するため、あるインターフェイスから別のインターフェイスへのデータ転送は禁止されています。外部 ID ストアはイーサネット 0 インターフェイスだけでサポートされます。ACS 5.8.1 では、RADIUS および TACACS+ プロキシ機能用にも複数のネットワーク インターフェイスがサポートされます。

シスコでは、ACS で異なるインターフェイスごとに異なるサブネットの IP アドレスを使用することを推奨しています。ACS で異なるインターフェイスに同じサブネットの IP アドレスを使用すると、同じサブネットの IP アドレスに対して同じ MAC アドレスをもつ ARP 応答を送信することになります。この推奨は NIC ボンディング機能には適用されません。イーサネット 0 とイーサネット 1 インターフェイスの両方を同じサブネットから IP アドレスを使用して設定すると、CLI および ACS 管理インターフェイスにイーサネット 0 とイーサネット 1 の両方のインターフェイスからアクセスできるようになります。そのため、イーサネット インターフェイス 0 のみを使用して ACS（CLI および ACS Web インターフェイス）を制限するには、イーサネット 0 とイーサネット 1 インターフェイスの IP アドレスが別のサブネットから設定される必要があります。

複数のネットワーク インターフェイスの設定

デフォルトでは、イーサネット インターフェイス 0 は ACS に割り当てられた IP アドレスを取得します。一方、他のイーサネット ポートには IP アドレスを手動で設定する必要があります。

イーサネット ポート用の IP アドレスを設定するには、次の手順を実行します。

1. CLI ユーザ名とパスワードを使用して、ACS CLI にログインします。
2. **config t** と入力して ACS CLI のコンフィギュレーション モードを開始します。
3. **interface GigabitEthernet *number*** コマンドを入力します。
4. インターフェイスをアップにするには、**no shutdown** コマンドを入力します。
5. **ip address *ip address subnet mask*** コマンドを入力します。

   次のメッセージがコンソールに表示されます。

   Changing the IP may result in undesired side effects on any installed application(s).

   Are you sure you want to proceed? Y/N [N]:
6. **Y** と入力します。

指定したインターフェイスが、指定の IP アドレスに設定されます。

ACS は自動的に再起動します。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

IPv6 対応のネットワークでは、イーサネット インターフェイス 0 はデュアル スタックのインターフェイスとして機能できますが、IPv4 アドレスを設定する必要があります。イーサネット 0 以外のイーサネット インターフェイスでは、IPv6 アドレスまたは IPv4 アドレスのいずれかまたは両方を使用します。他のイーサネット ポートで IPv4 アドレスを使用するには、上記の **ip address** *Ipv4 address ip-mask* コマンドを使用して IPv4 アドレスを設定する必要があります。

注: ACS 5.8.1 は、IPv4 と IPv6 のデュアル スタック ネットワーキングをサポートしていますが、純粋な IPv6 ネットワークはサポートしていません。

イーサネット インターフェイスのボンディング

ACS は、2 つの物理インターフェイスから 1 つの仮想インターフェイスへのボンディングをサポートしています。この機能は、ネットワーク インターフェイス カード（NIC）のボンディングと呼ばれます。2 つの物理インターフェイスから 1 つの仮想インターフェイスへのこのボンディングは、2 つのインターフェイスのいずれかがダウンしたときに、ACS がアクセス要求を処理するのを支援します。ボンドで 1 つの物理インターフェイスがダウンすると、同じボンドのもう一方の物理インターフェイスが他方のバックアップとして機能し、このボンディングに送信されるすべての要求を処理します。ACS の NIC ボンディング機能は、もう一方のインターフェイスがダウンした場合に 1 つの物理インターフェイスのバックアップのみを提供します。ロード バランシングなどの NIC ボンディングの他の一般的な機能は、サポートされていません。ACS 5.8.1 には 6 つのイーサネット インターフェイスが使用可能なので、3 つのボンドを作成できます。

ACS での NIC ボンディングの作成に関する注意事項:

- ボンド 0: イーサネット インターフェイス 0 とイーサネット インターフェイス 1 を組み合わせて、ボンド 0 を作成できます。イーサネット インターフェイス 0 と 1 は、ボンド 0 のスレーブとして動作します。ボンド 0 では、イーサネット インターフェイス 0 はプライマリ スレーブであり、イーサネット インターフェイス 1 はセカンダリ スレーブです。そのため、イーサネット インターフェイス 0 がダウンすると、イーサネット インターフェイス 1 がイーサネット インターフェイス 0 のバックアップとして機能し、すべての要求を処理します。イーサネット インターフェイス 1 は、ボンド 0 のプライマリ スレーブにすることはできません。ボンド 0 はイーサネット インターフェイス 0 の IP アドレスを取得し、イーサネット インターフェイス 1 の IP アドレスを削除します。ボンド 0 はイーサネット インターフェイス 0 の MAC アドレスを取得し、同じアドレスをイーサネット インターフェイス 1 に割り当てます。

- ボンド 1: イーサネット インターフェイス 2 とイーサネット インターフェイス 3 を組み合わせて、ボンド 1 を作成できます。イーサネット インターフェイス 2 と 3 は、ボンド 1 のスレーブとして動作します。ボンド 1 では、イーサネット インターフェイス 2 はプライマリ スレーブであり、イーサネット インターフェイス 3 はセカンダリ スレーブです。そのため、イーサネット インターフェイス 2 がダウンすると、イーサネット インターフェイス 3 がイーサネット インターフェイス 2 のバックアップとして機能し、すべての要求を処理します。イーサネット インターフェイス 3 は、ボンド 1 のプライマリ スレーブにすることはできません。ボンド 1 はイーサネット インターフェイス 2 の IP アドレスを取得し、イーサネット インターフェイス 3 の IP アドレスを削除します。ボンド 1 はイーサネット インターフェイス 2 の MAC アドレスを取得し、同じアドレスをイーサネット インターフェイス 3 に割り当てます。

- ボンド 2: イーサネット インターフェイス 4 とイーサネット インターフェイス 5 を組み合わせて、ボンド 2 を作成できます。イーサネット インターフェイス 4 と 5 は、ボンド 2 のスレーブとして動作します。ボンド 2 では、イーサネット インターフェイス 4 はプライマリ スレーブであり、イーサネット インターフェイス 5 はセカンダリ スレーブです。そのため、イーサネット インターフェイス 4 がダウンすると、イーサネット インターフェイス 5 がイーサネット インターフェイス 4 のバックアップとして機能し、すべての要求を処理します。イーサネット インターフェイス 5 は、ボンド 2 のプライマリ スレーブにすることはできません。ボンド 2 はイーサネット インターフェイス 4 の IP アドレスを取得し、イーサネット インターフェイス 5 の IP アドレスを削除します。ボンド 2 はイーサネット インターフェイス 4 の MAC アドレスを取得し、同じアドレスをイーサネット インターフェイス 5 に割り当てます。

- 前述のように、ACS ではボンド 0、ボンド 1、ボンド 2 の 3 つのボンドのみ持つことができます。インターフェイス 1 と 2、3 と 4、1 と 5 をボンディングすることはできません。イーサネット 2 またはイーサネット 3 インターフェイスをイーサネット 0 のバックアップ インターフェイスとすることはできません。他も同様です。

- 1 つのボンド内では、関わっている 2 つの物理イーサネット インターフェイスが同じサブネットにある必要があります。異なるサブネットからイーサネット インターフェイスとのインターフェイス ボンディングを作成できません。ボンド 0 を作成する前に、イーサネット インターフェイス 0 に IPv4 アドレスが割り当てられている必要があります。同様に、IPv4 または IPv6 アドレスがイーサネット 2 インターフェイスに割り当てられずに、ボンド 1 を作成できません。
- イーサネット インターフェイス 0 は管理インターフェイス、ランタイム インターフェイスの両方として動作しますが、他のインターフェイスはランタイム インターフェイスとしてのみ動作します。ACS では、ボンド 0 を作成し、他のイーサネット インターフェイスをそのままの状態にしておくことができます。この場合、ボンド 0 は管理インターフェイス、ランタイム インターフェイスの両方として機能し、他のイーサネットはランタイム インターフェイスとなります。ボンド 0、ボンド 1、ボンド 2 の 3 つのボンドを作成すると、ボンド 0 は管理インターフェイス、ランタイム インターフェイスの両方として機能し、ボンド 1、ボンド 2 はランタイム インターフェイスとなります。
- ボンディングでは、プライマリ スレーブ インターフェイスの IP アドレスを変更できます。ボンディングはプライマリ スレーブの IP アドレスを取得するので、新しい IP アドレスがボンディング インターフェイスに割り当てられます。
- インターフェイスのボンディングを中断すると、ボンディング インターフェイスに割り当てられた IP アドレスは、プライマリ スレーブ インターフェイスに再び割り当てられます。IP アドレスがなければ、セカンダリ スレーブはダウンします。セカンダリ スレーブに対して IP アドレスを手動で設定する必要があります。
- 分散導入で ACS インスタンスに対してインターフェイス ボンディングを設定する場合、この導入から ACS インスタンスの登録を解除し、インターフェイスのボンディングを設定してから、再び ACS インスタンスをこの導入に登録します。
- **show running-config** および **show interface** コマンドを使用して、ボンディング インターフェイスの情報を参照してください。

インターフェイス ボンディングの設定

ボンド 0 を作成するには、次の手順を実行します。

1. CLI ユーザ名とパスワードを使用して、ACS CLI にログインします。
2. **config t** と入力してコンフィギュレーション モードを開始します。
3. **interface GigabitEthernet 0** コマンドを入力します。
4. インターフェイスをアップにするには、**no shutdown** コマンドを入力します。
5. **backup interface GibabitEthernet 1** コマンドを入力します。

   次のメッセージがコンソールに表示されます。

   WARN: IP address of interface eth1 will be removed once NIC bonding is enabled.

   Configuring backup interface may result in undesired side effects on any installed application(s).

   Are you sure you want to proceed? Y/N [N]:

6. **Y** と入力します。

   次のメッセージがコンソールに表示されます。

```
Shutting down ntpd:                                        [  OK  ]
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
Bonding Interface was modified.
ACS is restarting and a new HTTP certificate will be generated.
Stopping ACS.
Stopping Management and View........
```

   ボンド 0 が設定されました。

   ACS は自動的に再起動します。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

ボンド 1 を作成するには、次の手順を実行します。

1. CLI ユーザ名とパスワードを使用して、ACS CLI にログインします。
2. **config t** と入力してコンフィギュレーション モードを開始します。
3. **interface GigabitEthernet 2** コマンドを入力します。
4. インターフェイスをアップにするには、**no shutdown** コマンドを入力します。
5. **backup interface GigabitEthernet 3** コマンドを入力します。

   次のメッセージがコンソールに表示されます。

   WARN: IP address of interface eth3 will be removed once NIC bonding is enabled.

   Configuring backup interface may result in undesired side effects on any installed application(s).

   Are you sure you want to proceed? Y/N [N]:
6. **Y** と入力します。

   次のメッセージがコンソールに表示されます。

```
Shutting down ntpd:                                        [  OK  ]
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
Bonding Interface was modified.
ACS is restarting and a new HTTP certificate will be generated.
Stopping ACS.
Stopping Management and View........
```

   ボンド 1 が設定されました。

   ACS は自動的に再起動します。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

ボンド 2 を作成するには、次の手順を実行します。

1. CLI ユーザ名とパスワードを使用して、ACS CLI にログインします。
2. **config t** と入力してコンフィギュレーション モードを開始します。
3. **interface GigabitEthernet 4** コマンドを入力します。
4. インターフェイスをアップにするには、**no shutdown** コマンドを入力します。
5. **backup interface GigabitEthernet 5** コマンドを入力します。

   次のメッセージがコンソールに表示されます。

   WARN: IP address of interface eth5 will be removed once NIC bonding is enabled.

   Configuring backup interface may result in undesired side effects on any installed application(s).

   Are you sure you want to proceed? Y/N [N]:

6. **Y** と入力します。

   次のメッセージがコンソールに表示されます。

```
Shutting down ntpd:                                        [  OK  ]
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
Bonding Interface was modified.
ACS is restarting and a new HTTP certificate will be generated.
Stopping ACS.
Stopping Management and View........
```

   ボンド 2 が設定されました。

   ACS は自動的に再起動します。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

NIC ボンドの削除

backup interface コマンドの **no** 形式を使用して、ACS から NIC ボンディングを削除します。

ボンド 0 を削除するには、次の手順を実行します。

1. CLI ユーザ名とパスワードを使用して、ACS CLI にログインします。
2. **config t** と入力してコンフィギュレーション モードを開始します。
3. **interface GigabitEthernet 0** コマンドを入力します。
4. **no backup interface GigabitEthernet 1** コマンドを入力します。

   次のメッセージがコンソールに表示されます。

   Removing backup interface configuration may result in undesired side effects on any installed application(s).

   Are you sure you want to proceed? Y/N [N]:

5. **Y** と入力します。

   次のメッセージがコンソールに表示されます。

```
Shutting down ntpd:                                        [  OK  ]
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
Bonding Interface was modified.
ACS is restarting and a new HTTP certificate will be generated.
ACS is not running.
To start ACS type 'application start acs'.
Starting ACS ..........
To verify that ACS processes are running, use the
'show application status acs' command.
```

   ボンド 0 が削除されました。

   ACS は自動的に再起動します。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

ボンド 1 を削除するには、次の手順を実行します。

1. CLI ユーザ名とパスワードを使用して、ACS CLI にログインします。
2. **config t** と入力してコンフィギュレーション モードを開始します。
3. **interface GigabitEthernet 2** コマンドを入力します。

4. **no backup interface GigabitEthernet 3** コマンドを入力します。

   次のメッセージがコンソールに表示されます。

   Removing backup interface configuration may result in undesired side effects on any installed application(s).

   Are you sure you want to proceed? Y/N [N]:

5. **Y** と入力します。

   次のメッセージがコンソールに表示されます。

```
Shutting down ntpd:                                        [  OK  ]
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
Bonding Interface was modified.
ACS is restarting and a new HTTP certificate will be generated.
ACS is not running.
To start ACS type 'application start acs'.
Starting ACS..........
To verify that ACS processes are running, use the
'show application status acs' command.
```

   ボンド 1 が削除されました。

   ACS は自動的に再起動します。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

ボンド 2 を削除するには、次の手順を実行します。

1. CLI ユーザ名とパスワードを使用して、ACS CLI にログインします。
2. **config t** と入力してコンフィギュレーション モードを開始します。
3. **interface GigabitEthernet 4** コマンドを入力します。
4. **no backup interface GigabitEthernet 5** コマンドを入力します。

   次のメッセージがコンソールに表示されます。

   Removing backup interface configuration may result in undesired side effects on any installed application(s).

   Are you sure you want to proceed? Y/N [N]:

5. **Y** と入力します。

   次のメッセージがコンソールに表示されます。

```
Shutting down ntpd:                                        [  OK  ]
ntpd: Synchronizing with time server:                      [  OK  ]
Starting ntpd:                                             [  OK  ]
Bonding Interface was modified.
ACS is restarting and a new HTTP certificate will be generated.
ACS is not running.
To start ACS type 'application start acs'.
Starting ACS..........
To verify that ACS processes are running, use the
'show application status acs' command.
```

   ボンド 2 が削除されました。

   ACS は自動的に再起動します。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

コンソールの接続

警告:雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

CSACS-1121 シリーズ アプライアンスには、コンソール端末をアプライアンスに接続するための DCE モードのコンソール ポートがあります。アプライアンスのコンソール ポートでは、DB-9 シリアル コネクタが使用されています。

CSACS-1121 シリーズ アプライアンス上のコンソール ポートには、EIA/TIA-232 非同期シリアル(DB-9)コネクタが含まれています。このシリアル コンソール コネクタ(ポート)を使用することで、端末(ターミナル エミュレーション ソフトウェアが動作する PC か ASCII 端末)をコンソール ポートに接続し、アプライアンスにローカルにアクセスできます。

ターミナル エミュレーション ソフトウェアが動作する PC をコンソール ポートに接続するには、両端が DB-9 メスのストレート ケーブルを使用します。

ASCII 端末をコンソール ポートに接続するには、片方が DB-9 メスでもう一方が DB-25 オスのストレート ケーブルと、DB-25 メスから DB-25 メスへの変換アダプタを使用します。

端末またはターミナル エミュレーション ソフトウェアが動作する PC を、CSACS-1121 シリーズ アプライアンスのコンソール ポートに接続するには、次の手順を実行します。

1. ストレート ケーブルを使用して端末をコンソール ポートに接続します。
2. 端末またはターミナル エミュレーション ソフトウェアを、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、ハードウェア フロー制御なしに設定します。

シリアル(コンソール)ポート コネクタ

CSACS 1121 シリーズ アプライアンスでは、1 個のシリアル ポート コネクタが、アプライアンスの背面パネルにあります。

図 10(16 ページ) に、アプライアンスの背面パネルにある 9 ピン、オス D シェル シリアル ポート コネクタのピン番号の割り当てを示します。これらのピン番号の割り当ては、RS-232-C で定義されており、業界標準に準拠しています。

図 10　シリアル ポート コネクタ

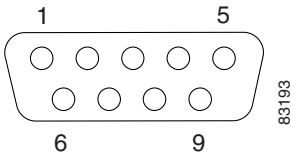


表 5(16 ページ)にシリアル(コンソール)ポートのピン配置を示します。

表 5　DB-9 シリアル(コンソール)ポートのピン配置

シリアル ポート ピン	信号	説明
1	DCD	データキャリア検知
2	RXD	受信データ
3	TXD	送信データ
4	DTR	データ ターミナル レディ
5	GND	信号アース
6	DSR	データ セット レディ
7	RTS	送信要求
8	CTS	Clear To Send
9	RI	リング インジケータ

キーボードとビデオ モニタの接続

警告:雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

ここでは、キーボードとビデオ モニタを CSACS-1121 シリーズ アプライアンスに接続するための方法について説明します。

キーボードとビデオ モニタの代わりに、シリアル コンソールを使用して CSACS-1121 アプライアンスに接続できます。

CSACS-1121 アプライアンスはマウスをサポートしていません。

CSACS-1121 には、アプライアンスの前面と背面に USB ポートがあり、キーボードとビデオ モニタを接続するために使用できます。

キーボードとビデオ モニタをアプライアンスに接続するには、次の手順を実行します。

1. アプライアンスの電源がオフになっていることを確認します。
2. キーボード ケーブルの端を、アプライアンスの背面パネルにある PS/2(キーボード)ポートに接続します。
3. ビデオ モニタ ケーブルの端を、アプライアンスの背面パネルにある PS/2(ビデオ モニタ)ポートに接続します。
4. アプライアンスの電源をオンにします。

ケーブル管理

ケーブル管理は、アプライアンスの設定の中で、最も外観に関係する作業です。しかし、ケーブル管理には時間がかかるため、放置しがちです。

今日の装置ラックは、従来よりも多くの装置を収納するようになっています。このため、ラックの内部と外部で整然としたケーブル管理を行う必要性が高まっています。ケーブル管理が適切でないと、ケーブルが損傷したりケーブルの追加や変更に時間がかかったりするだけでなく、重要な通気やアクセスが妨げられます。これらの問題により、装置のパフォーマンスが低下したり、ダウンタイムが長くなったりするおそれがあります。

ケーブル管理を扱うためのソリューションは多数あります。単純なケーブル管理リングから、垂直または水平収納容器、樋やはしごに至るまで、さまざまなソリューションがあります。

すべての CSACS-1121 シリーズ アプライアンス ケーブルは、ケーブル同士や装置の他の部分と干渉しないように、適切に整理する必要があります。各地の慣習に従って、アプライアンスに接続されているケーブルを適切に整理してください。

設置手順を続行するには、次のセクションCSACS-1121 シリーズ アプライアンスの電源投入(17 ページ)に進んでください。

CSACS-1121 シリーズ アプライアンスの電源投入

警告:電源コードが接続されている場合、電源に触れないでください。電源スイッチを備えたシステムの場合、電源スイッチがオフになっていても、電源コードが接続されていれば、電源装置内部に入力電圧がかかっています。電源スイッチのないシステムの場合、電源コードが接続されていれば、電源装置内部に入力電圧がかかっています。ステートメント 4

警告:この装置は接地されることを前提としています。通常の使用時にホストが接地されていることを確認してください。ステートメント 39

ここでは、次の項目について説明します。

- 電源投入のためのチェックリスト(18 ページ)
- 電源投入手順(18 ページ)
- LED の確認(19 ページ)

電源投入のためのチェックリスト

次の状態では、CSACS-1121 シリーズ アプライアンスの電源を投入する準備が完了しています。

- アプライアンスがしっかりとマウントされている。
- 電源、ネットワーク、インターフェイス ケーブルが適切に接続されている。

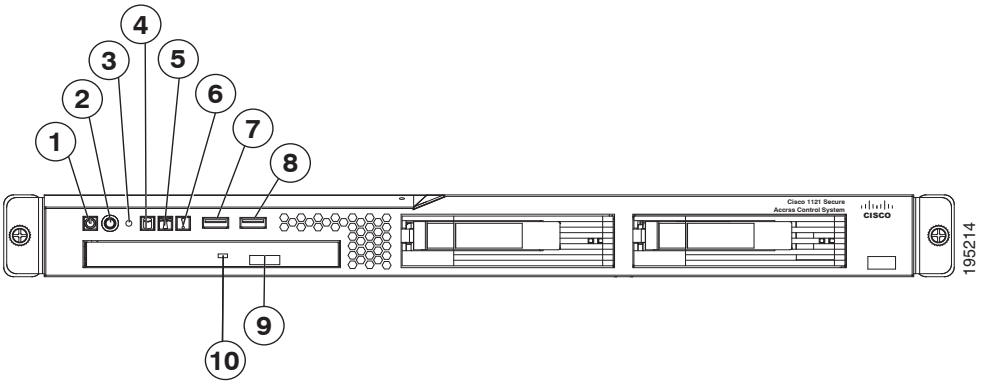
電源投入手順

CSACS-1121 シリーズ アプライアンスの電源を投入し、その初期化とセルフテストを確認するには、次の手順を実行します。手順が完了すると、アプライアンスを設定する準備ができます。

1. 安全に関するガイドライン（1 ページ）の情報を確認してください。
2. AC 電源コードを、アプライアンスの背面にある電源コード レセプタクルに差し込みます（図 7（7 ページ） の 1 番を参照）。
3. 電源コードの他方の端を、設置場所の電源に接続します。
4. アプライアンスの前面にある電源ボタンを押します（図 11（18 ページ） の 2 番を参照）。

   アプライアンスが起動を開始します。オペレーティング システムが起動したら、基本的なソフトウェアの設定を初期化できます。設定手順については、ソフトウェア インストール ガイドまたはユーザ ガイドを参照してください。

図 11　CSACS-1121 シリーズ アプライアンスの正面図



次の表で、図 11（18 ページ） の各コンポーネントについて説明します。

1	アプライアンス電源 LED	6	システム エラー LED
2	電源制御ボタン	7	USB 1 コネクタ
3	リセットボタン	8	USB 2 コネクタ
4	ハードディスク ドライブ アクティビティ LED	9	CD 取り出しボタン
5	ロケータ LED	10	CD ドライブ アクティビティ LED

LED の確認

CSACS-1121 シリーズ アプライアンスが起動したら、前面パネルの LED を観察します。次の LED は、電源、アクティビティ、ステータス情報を提供します。

CSACS-1121 アプライアンスの前面パネル LED

- アプライアンス電源、緑:
  - 電源がオンの場合に点灯。
  - 電源がオフか、動作電圧内でエラー条件が検出された場合に消灯。
- ハードディスク アクティビティ、緑:
  - アプライアンス ソフトウェアが起動し、アプライアンスが動作可能な場合に点灯。
  - アプライアンスがまだ起動していないか、起動プロセスでエラー条件が検出された場合に消灯。

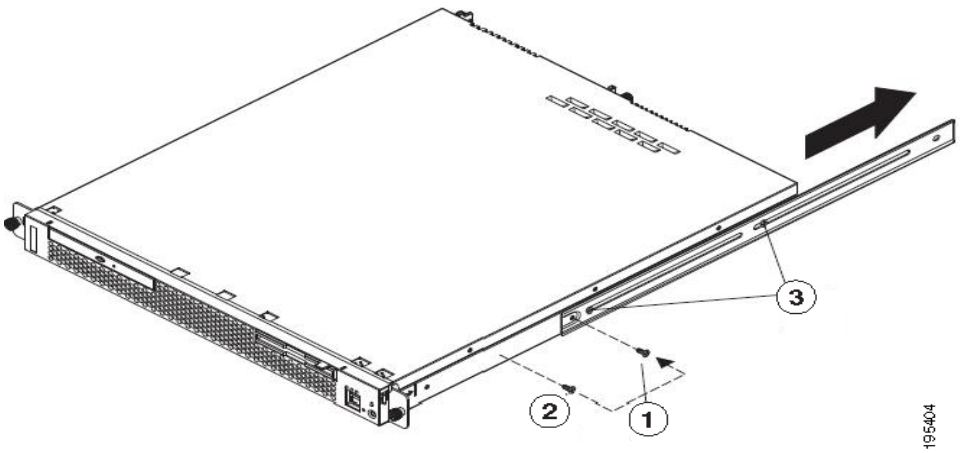
LED の詳細については、トラブルシューティング（1 ページ）を参照してください。

ラック キャビネットの輸送の準備

CSACS-1121 シリーズ アプライアンスを、サーバが取り付けられた状態で別の場所に輸送するには、次の手順を実行します。

1. 大きなネジ（図 12（19 ページ） を参照）を取り外し、廃棄します。
2. 前面ネジを取り外して保管します。
3. 残り 2 本の背面のネジを緩めます。
4. レールを一杯に伸ばし、保管しておいたネジを大きなネジがあった場所に挿入します。
5. すべてのネジを締めてレールを固定します。
6. 反対側のレールに対してステップ 1.大きなネジ（図 12（19 ページ） を参照）を取り外し、廃棄します。（19 ページ） ～ 5.すべてのネジを締めてレールを固定します。（19 ページ） を繰り返します。

図 12　ラック キャビネットの輸送の準備



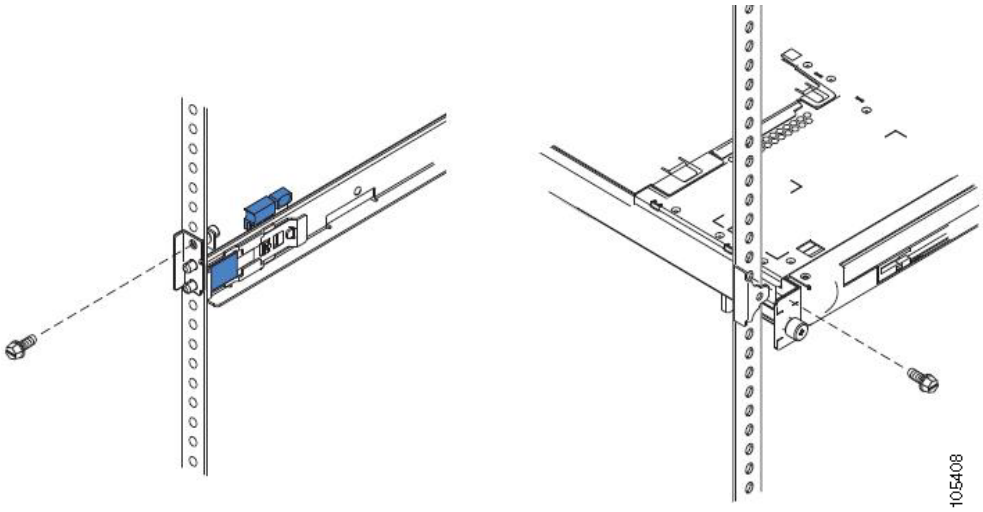
次の表で、図 12（19 ページ）の各コンポーネントについて説明します。

1	大きなネジ	3	2 本の背面ネジ
2	前面ネジ		

7. 次のようにしてサーバをラックに固定する必要があります。
   a. 必要に応じて、サーバの背面からケーブルを外します。
   b. サーバをラックの外に 150 mm（6 インチ）スライドさせ、M6 ネジを各スライド レールに挿入します。
   c. M6 ネジでサーバをラック キャビネットに固定します。図 13（20 ページ）を参照してください。
8. レールがラック キャビネットの背面に向けて完全に伸びていることを確認します。

   スライド レールから輸送用ブラケットを取り外してある場合は、サーバが取り付けられた状態でラック キャビネットを輸送する前に、輸送用ブラケットを再度取り付ける必要があります。図 6（7 ページ）に示した手順と逆の手順を実行して、輸送用ブラケットを取り付けます。

図 13　ラック キャビネットを別の場所に移動するための準備



CSACS-1121 シリーズ アプライアンスの取り外しまたは交換

警告：電源スイッチのあるシステムの作業を行う前に電源をオフにし、電源コードを抜いてください。ステートメント 1

警告：本製品の最終処分の際は、各国の法律や規制に従ってください。ステートメント 1040

ここでは、次の項目について説明します。

- CSACS-1121 シリーズ アプライアンスの取り外し（21 ページ）
- CSACS-1121 シリーズ アプライアンスの交換（21 ページ）

CSACS-1121 シリーズ アプライアンスの取り外し

CSACS-1121 シリーズ アプライアンスをネットワークから取り除くには、次の手順を実行します。

1. アプライアンスの電源をオフにします。
2. 電源コードとネットワーク ケーブルを外します。
3. アプライアンスをラックから物理的に取り外します。

   アプライアンスはネットワーク上で定期的に通信しているため、ネットワークは、アプライアンスが応答しなくなったことを検出すると、アプライアンスへの要求の送信を停止します。この変化はユーザに見えます。

注：別のアプライアンスがネットワークに接続されている場合、ネットワークは別のアプライアンスに要求を送信し続けます。

CSACS-1121 シリーズ アプライアンスの交換

アプライアンスを交換するには、次の手順を実行します。

1. アプライアンスをネットワークから取り除きます。
2. 以前のアプライアンスに対して使用したのと同じ設置手順を使用して、新しいアプライアンスを設置します。
3. 取り除いたアプライアンスに使用したのと同じ設定パラメータを使用して、新しいアプライアンスを設定します。

CSACS-1121 を使用した Cisco Secure Access Control System のインストールと設定

この章では、CSACS-1121 と ACS 5.8.1 サーバをインストールおよび初期設定する方法について説明します。

- CSACS-1121 シリーズ アプライアンスを使用したインストール（1 ページ）
- Cisco Secure ACS 5.8.1 ISO イメージのダウンロード（2 ページ）
- ACS サーバのインストール（2 ページ）
- 管理者パスワードのリセット（6 ページ）
- ACS サーバの再イメージ化（6 ページ）

CSACS-1121 シリーズ アプライアンスを使用したインストール

CSACS-1121 アプライアンスには、ACS 5.8.1 ソフトウェアがあらかじめインストールされています。ここでは、インストール プロセスの概要と、ACS をインストールする前に実行する必要がある作業について説明します。

ACS 5.8.1 のインストールを開始する前に、次の作業を実行する必要があります。

1. 箱を開けて内容を確認します。開梱と出荷内容の確認（9 ページ）を参照してください
2. Cisco 1121 Secure Access Control System ハードウェアの導入（1 ページ）を参照してください
3. Cisco 1121 Secure Access Control System ハードウェアの設置準備（1 ページ）にある、一般的な注意事項と安全に関する警告を読みます。
4. アプライアンスをラックに取り付けます。Cisco 1121 Secure Access Control System ハードウェアの設置（1 ページ）を参照してください
5. CSACS-1121 をネットワークとアプライアンス コンソールに接続します。ケーブルの接続（7 ページ）を参照してください
6. CSACS-1121 アプライアンスの電源をオンにします。CSACS-1121 シリーズ アプライアンスの電源投入（17 ページ）を参照してください
7. CLI プロンプトで **setup** コマンドを実行し、ACS サーバの初期設定を行います。セットアップ プログラムの実行（2 ページ）を参照してください。

Cisco Secure ACS 5.8.1 ISO イメージのダウンロード

Cisco.com から Cisco Secure ACS 5.8.1 ISO イメージをダウンロードできます。

1. http://www.cisco.com/go/acs にアクセスします。このリンクにアクセスするには、有効な Cisco.com ログイン クレデンシャルを所有している必要があります。
2. [Download Software] をクリックします。

Cisco.com ページに Cisco Secure ACS リリース 5.8.1 ソフトウェア イメージが表示されます。インストールおよび初期設定が完了したら、すべての Cisco ACS サービスのテストを実行できます。

注:ACS 5.x ソフトウェア イメージを Cisco.com からダウンロードできるのは、以前のバージョンの ACS 5.x ソフトウェアについて有効な Software Application Support(SAS)契約を結んでいる場合だけです。以前のバージョンで有効な SAS 契約を結んでいない場合は、Cisco.com のソフトウェア イメージを特定のカスタマー アカウントに公開するには、販売エンジニア(SE)、アカウント マネージャ(AM)、またはシスコ パートナーにお問い合わせください。

ACS サーバのインストール

ここでは、CSACS-1121 シリーズ アプライアンスに ACS をインストールする方法について説明します。

ここでは、次の項目について説明します。

- セットアップ プログラムの実行(2 ページ)
- インストール プロセスの確認(5 ページ)

セットアップ プログラムの実行

ここでは、ACS サーバをインストールするためのセットアップ プロセスについて説明します。

セットアップ プログラムでは、必要なパラメータの入力を求める、対話型のコマンドライン インターフェイス(CLI)が起動されます。

管理者は、コンソールまたはダム端末とセットアップ プログラムを使用して、ACS 5.8.1 サーバの初期ネットワークを設定し、初期管理者資格情報を設定します。セットアップ プロセスは一度だけ実行する設定作業です。

ACS サーバをインストールするには、次の手順を実行します。

1. アプライアンスの電源をオンにします。

   次のセットアップ プロンプトが表示されます。

   ```
   Please type 'setup' to configure the appliance
   localhost login:
   ```

2. ログイン プロンプトで **setup** と入力し、Enter を押します。

   コンソールにパラメータのセットが表示されます。表 1(3 ページ) の説明に従ってパラメータを入力します。

注:セットアップ プロセスは、最後のセットアップ値を入力する前に、Ctrl+C を押すことでいつでも中断できます。

表 1　ネットワーク設定パラメータ

プロンプト	デフォルト	条件	説明
ホスト名	*localhost*	最初の文字は ASCII 文字である必要があります。 長さは 3 ～ 15 文字である必要があります。 有効な文字は、英数字（A ～ Z、a ～ z、0 ～ 9）とハイフン（-）で、最初の文字はアルファベットである必要があります。 **注**：AD ID ストアを使用し、同じ名前のプレフィックスで複数の ACS インスタンスを設定する場合は、ホスト名として最大 15 文字を使用して AD 機能が影響を受けないようにします。	ホスト名を入力します。
IPV4 IP Address	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	IP アドレスを入力します。
IPv4 Netmask	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なネットマスクを入力します。
IPv4 Gateway	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なデフォルト ゲートウェイを入力します。
ドメイン名	なし。ネットワーク固有	IP アドレスは入力できません。 有効な文字は、ASCII 文字、数値、ハイフン（-）、およびピリオド（.）です。	ドメイン名を入力します。
IPv4 Primary Name Server Address	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なネーム サーバ アドレスを入力します。
Add another nameserver	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。 **注**：ACS CLI から最大 3 つのネーム サーバを設定できます。	複数のネーム サーバを設定するには、**y** と入力します。
NTP サーバ	time.nist.gov	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレス、またはドメイン ネーム サーバにする必要があります。 **注**：ACS CLI から最大 3 つの NTP サーバを設定できます。	有効なドメイン ネーム サーバまたは IPv4 アドレスを入力します。
タイムゾーン	UTC	有効なローカル タイム ゾーンである必要があります。	有効なタイム ゾーンを入力します。

表 1　ネットワーク設定パラメータ（続き）

プロンプト	デフォルト	条件	説明
SSH サービス	なし。ネットワーク固有	なし	SSH サービスを有効にするには、**y** と入力します。
ユーザ名	admin	最初の管理ユーザの名前です。デフォルトを受け入れるか、新しいユーザ名を入力します。 ユーザ名は 3 ～ 8 文字の英数字（A ～ Z、a ～ z、0 ～ 9）にする必要があります。	ユーザ名を入力します。
Admin パスワード	なし	デフォルトのパスワードはありません。パスワードを入力します。 パスワードは最低 6 文字で、小文字、大文字、数字がそれぞれ 1 つ以上含まれている必要があります。 また、次の点に注意してください。 ■ 初期設定で設定したアカウントのユーザとパスワードの情報は大切に保管してください。 ■ これらのクレデンシャルを使用すると、ACS ハードウェア、CLI、アプリケーションを管理者として完全に制御できるため、忘れないようにして保護します。 ■ 管理者のクレデンシャルを紛失した場合、ACS 5.8.1 の Installation and Recovery DVD を使用してパスワードをリセットできます。	パスワードを入力します。

コンソールで、次のパラメータを入力するよう求められます。

```
localhost login: setup
Enter hostname[]: acs-server-1
Enter IP address[]: a.b.c.d
Enter IP default netmask[]: 255.255.255.255
Enter IP default gateway[]: a.b.c.d
Enter default DNS domain[]: mycompany.com
Enter primary nameserver[]: a.b.c.d
Add secondary nameserver? Y/N : n
Add primary NTP server [time.nist.gov]: a.b.c.d
Add secondary NTP server? Y/N : n
Enter system timezone[UTC]:
Enable SSH service? Y/N [N] : y
Enter username [admin]: admin
Enter password:
Enter password again:
Pinging the gateway...
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing acs...
Generating configuration...
Rebooting...
```

ACS サーバのインストールが完了すると、システムは自動的に再起動します。

この時点で、セットアップ プロセスで設定した CLI ユーザ名とパスワードを使用して ACS にログインできるようになります。

注: このユーザ名とパスワードを使用して ACS にログインできるのは、CLI を通じてだけです。

注: ACS 5.8.1 の初期設定では、サーバに IPv4 アドレスを設定する必要があります。サーバの IPv6 IP アドレスは、初期設定完了後にのみ設定できます。

注: ACS 5.8.1 は、IPv4 と IPv6 のデュアル スタック ネットワーキングをサポートしていますが、純粋な IPv6 ネットワークはサポートしていません。

インストール プロセスの確認

インストール プロセスが正しく完了したことを確認するには、次の手順を実行します。

1. システムが再起動したら、ログイン プロンプトでセットアップ時に設定したユーザ名を入力し、Enter を押します。
2. パスワード プロンプトで、セットアップ時に設定したパスワードを入力し、Enter を押します。
3. アプリケーションが適切にインストールされていることを確認するために、**show application** と入力し、Enter を押します。

   コンソールに次のメッセージが表示されます。

```
<name>          <Description>
acs Cisco Secure Access Control System 5.8.1
```

4. システム プロンプトでインストールされているリリースと ACS のバージョンを確認するため、システム プロンプトで **show application version acs** と入力して Enter を押します。

   コンソールに次のメッセージが表示されます。

```
Cisco ACS VERSION INFORMATION

-----------------------------

Version: 5.8.1.4
Internal Build ID: B.462
```

注: このリリースの別のバージョンでは、Version と Internal Build ID が変更されている場合があります。

5. ACS プロセスのステータスを確認するために、システム プロンプトで **show application status acs** と入力し、**Enter** を押します。

   コンソールに次のメッセージが表示されます。

```
ACS role: PRIMARY
Process 'database'                running
Process 'management'              running
Process 'runtime'                 running
Process 'adclient'                running
Process 'ntpd'                    running
Process 'view-database'           running
Process 'view-jobmanager'         running
Process 'view-alertmanager'       running
Process 'view-collector'          running
Process 'view-logprocessor'       running
```

注: 最新の ACS パッチを入手し ACS を最新に保つには、http://software.cisco.com/download/navigator.html?i=rt を参照してください。

管理者パスワードのリセット

管理者パスワードを失ったためにシステムにログインできない場合は、ACS 5.8.1 Recovery DVD を使用して管理者パスワードをリセットできます。

管理者パスワードをリセットするには、次の手順を実行します。

1. アプライアンスの電源をオンにします。
2. ACS 5.8.1 Recovery DVD を挿入します。

   コンソールに次のメッセージが表示されます。

```
Welcome to Cisco Secure ACS 5.8.1 Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS 5.8.1 Installation (Keyboard/Monitor)
[2] Cisco Secure ACS 5.8.1 Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot:
```

   管理者パスワードをリセットするには、システム プロンプトで、キーボードとビデオ モニタを使用している場合は **3** と入力し、シリアル コンソール ポートを使用している場合は **4** と入力します。

   コンソールにパラメータのセットが表示されます。

3. 表 2(6 ページ) の説明に従ってパラメータを入力します。

表 2　パスワード リセット パラメータ

パラメータ	説明
Admin username	パスワードをリセットする管理者の番号を入力します。
Password	管理者の新しいパスワードを入力します。
Verify password	パスワードを再度入力します。
Save change & Reboot	保存するには **y** と入力します。

   コンソールに次のメッセージが表示されます。

```
Admin username:
[1]:admin
[2]:admin2
[3]:admin3
Enter number of admin for password recovery:1
パスワード(Password):
Verify password:
Save change&reeboot? [Y/N]:
```

ACS サーバの再イメージ化

ACS サーバを再イメージ化するには、次の手順を実行します。

1. アプライアンスの電源をオンにします。
2. ACS Recovery DVD を挿入します。

コンソールに次のメッセージが表示されます。

```
Welcome to Cisco Secure ACS 5.8.1 Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS 5.8.1 Installation (Keyboard/Monitor)
[2] Cisco Secure ACS 5.8.1 Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot:
```

3. コンソール プロンプトで、キーボードとビデオ モニタを使用している場合は **1** と入力し、シリアル コンソール ポートを使用している場合は **2** と入力して、Enter を押します。

   再イメージ化処理により既存の ADE-OS と ACS バージョンがアンインストールされ、最新バージョンがインストールされます。インストール手順については、セットアップ プログラムの実行（2 ページ）のセクションを参照してください。

法規制の遵守

法令準拠および安全性に関する情報については、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を参照してください。

法規制の遵守

Cisco SNS 3400 サーバ上の ACS 5.8.1

Cisco SNS-3415 および Cisco SNS-3495 ハードウェア アプライアンスの導入

この章では、Cisco Secure Access Control System（Cisco SNS-3415 および Cisco SNS-3495）ハードウェアの概要を紹介します。ここでは、アプライアンス ハードウェア、主なコンポーネント、コントロール、コネクタ、前面および背面パネルの LED インジケータについて説明します。

- 製品の概要（1 ページ）
- Cisco SNS 3415 および 3495 アプライアンスの LED インジケータ（4 ページ）
- 法規制の遵守（8 ページ）

製品の概要

この項では、Cisco SNS-3415 および Cisco SNS-3495 アプライアンスの電源要件、ラックマウント ハードウェア キット、および機能について説明します。

ここでは、次の項目について説明します。

- Cisco SNS-3415 および Cisco SNS-3495 アプライアンスの概要（1 ページ）
- Cisco SNS-3415 および Cisco SNS-3495 アプライアンスのハードウェア仕様（2 ページ）
- 製品シリアル番号の場所（4 ページ）
- Cisco Product Identification ツール（4 ページ）

Cisco SNS-3415 および Cisco SNS-3495 アプライアンスの概要

Cisco SNS-3415/3495 サーバは、Web サービスから分散データベースまで、広範囲のビジネス上の負荷に対応できるパフォーマンスおよび密度のために設計されています。

Cisco SNS-3415/3495 サーバの成功を反映させたエンタープライズ クラスの Cisco SNS-3415/3495 サーバは、1-RU フォーム ファクタの Cisco Unified Computing System ポートフォリオの機能を拡張します。パフォーマンス、効率の向上を実現する Intel Xeon E5-2600 プロセッサ製品ファミリを搭載することで、Cisco SNS-3415 サーバはこれらの機能を提供します。さらに、Cisco SNS-3415/3495 サーバは、最大 256 GB の RAM、8 台のドライブ、コンパクトなパッケージで卓越したレベルのサーバ密度とパフォーマンスを提供する 2 つの 1 GbE Lights-Out Management（LOM）ポートを提供します。

Cisco SNS-3415 および Cisco SNS-3495 アプライアンスのハードウェア仕様

表 1（2 ページ）では、Cisco SNS-3415 および Cisco SNS-3495 アプライアンスのハードウェア仕様について説明します。

表 1　Cisco SNS 3415 および Cisco SNS 3495 ハードウェアの概要

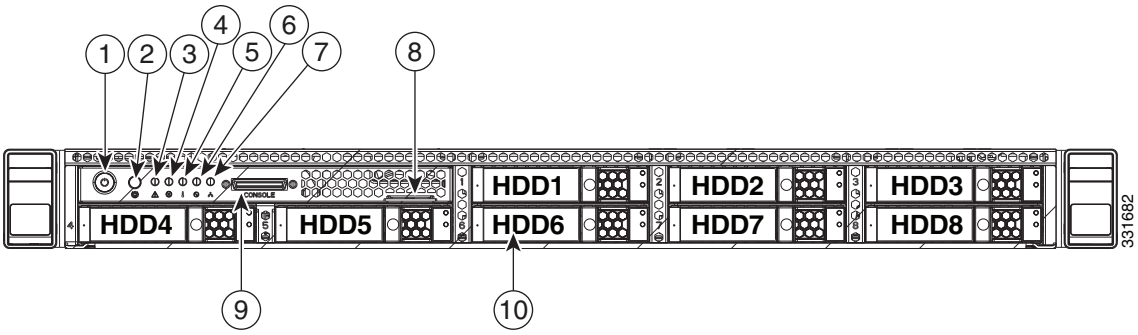
Cisco Secure ACS アプライアンス	ハードウェア仕様	図
Cisco SNS-3415-K9	■ Cisco UCS C220 M3 ■ シングル ソケット Intel E5-2609 2.4GHz CPU 合計 4 コア、合計 4 スレッド ■ 16 GB RAM ■ 600 GB ディスク x 1 ■ 組み込みソフトウェア RAID 0 ■ 4 GE ネットワーク インターフェイス ■ 物理的仕様、環境仕様、および電源仕様については、サーバの仕様（4 ページ）を参照してください。	■ 図 1Cisco SNS-3415/3495 アプライアンスの正面図（3 ページ） ■ 図 2Cisco SNS-3415/3495 アプライアンスの背面図（3 ページ）
Cisco SNS-3495-K9	■ Cisco UCS C220 M3 ■ デュアル ソケット Intel E5-2609 2.4GHz CPU 合計 8 コア、合計 8 スレッド ■ 32 GB RAM ■ 600 GB ディスク x 2 ■ RAID 0+1 ■ 4 GE ネットワーク インターフェイス ■ 物理的仕様、環境仕様、および電源仕様については、サーバの仕様（4 ページ）を参照してください。	■ 図 1Cisco SNS-3415/3495 アプライアンスの正面図（3 ページ） ■ 図 2Cisco SNS-3415/3495 アプライアンスの背面図（3 ページ）

注:ACS 5.8.1 は、Cisco SNS-3415-K9 のオプションの冗長電源装置をサポートします。

シャーシの正面図

図 1（3 ページ）に、Cisco SNS-3415/3495 サーバを示します。

図 1　Cisco SNS-3415/3495 アプライアンスの正面図

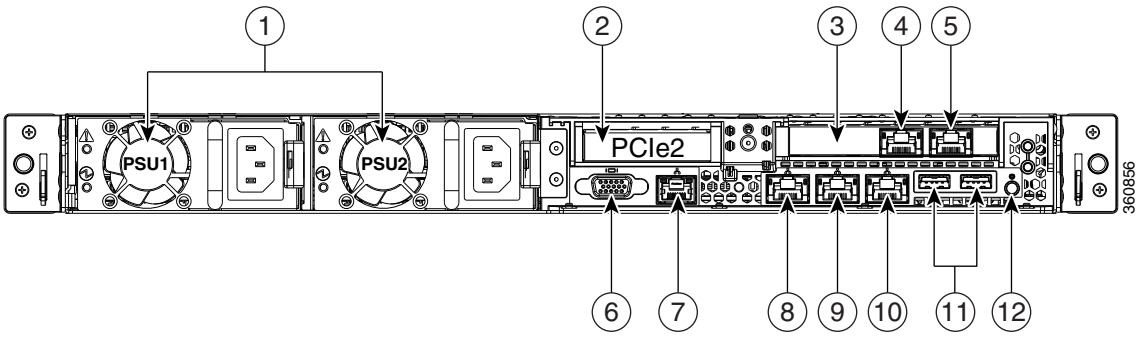


1	電源ボタン/電源ステータス LED	6	電源装置ステータス LED
2	ID ボタン/LED	7	ネットワーク リンク アクティビティ LED
3	システム ステータス LED	8	資産タグ（シリアル番号）
4	ファン ステータス LED	9	KVM コネクタ（USB × 2、VGA × 1、シリアル コネクタ × 1 が付いている KVM ケーブルを接続）
5	温度ステータス LED	10	ドライブ（最大 8 台のホットスワップ可能な 2.5 インチ ドライブ）

シャーシの背面図

図 2（3 ページ） に、Cisco SNS-3415 アプライアンスと Cisco SNS-3495 アプライアンスの背面パネルの外部機能を示します。

図 2　Cisco SNS-3415/3495 アプライアンスの背面図



1	電源（最大 2 台）	7	シリアル ポート（RJ-45 コネクタ）
2	スロット 2：ライザーのロープロファイル PCIe（Peripheral Component Interconnect Express）スロット（ハーフハイト、ハーフレングス、x16 コネクタ、x16 レーン幅）	8	CIMC へのアクセスに使用する 1 GB イーサネット専用管理ポート（M というラベル付き）
3	スロット 1：1 GB イーサネット ポートを含む PCIe1 カード（GigE2 および GigE3）	9	Cisco Secure ACS 管理通信用の 1 GB イーサネット ポート 1（GigE0）
4	1 GB イーサネット ポート 3（GigE2）	10	1 GB イーサネット ポート 2（GigE1）
5	1 GB イーサネット ポート 4（GigE3）	11	USB ポート
6	VGA ビデオ コネクタ	12	背面の識別ボタン

製品シリアル番号の場所

シリアル番号ラベルは、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの前面パネルのサーバの上部にあります。図 1（3 ページ） に、このラベルの場所を示します。

Cisco Product Identification ツール

Cisco 製品 ID（CPI）ツールは、シスコ製品のシリアル番号を取得する際に役立ちます。

オンラインまたは電話でサービスのリクエスト要求をする前に、CPI ツールを使用して製品のシリアル番号を検索します。このツールは、シスコのサポート Web サイトからアクセスできます。

ツールにアクセスする方法は、次のとおりです。

1. [Get Tools & Resources] リンクをクリックします。
2. [All Tools (A-Z)] タブをクリックします。
3. アルファベット順のドロップダウン リストから [Cisco Product Identification Tool] を選択します。

   このツールには、3 つの検索オプションがあります。

- 製品 ID またはモデル名による検索。
- シスコ モデルの参照。
- **show** コマンドで出力をコピー アンド ペーストして製品を特定。

  検索結果では、製品画像とともにシリアル番号ラベルの場所が強調表示されます。製品のシリアル番号ラベルのある場所を探し、サービスに問い合わせる前にその情報を記録します。

  CPI ツールは、次の URL からアクセスできます。

  http://tools.cisco.com/Support/CPI/index.do

  CPI ツールにアクセスするには、Cisco.com ユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

  http://tools.cisco.com/RPF/register/register.do

Cisco SNS 3415 および 3495 アプライアンスの LED インジケータ

この項では、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの前面および背面パネルのコントロール、ポート、および LED インジケータについて説明します。

ここでは、次の項目について説明します。

- Cisco SNS-3415/3495 アプライアンスの前面パネル ビュー（5 ページ）
- Cisco SNS-3415/3495 アプライアンスの背面パネル ビュー（6 ページ）
- 内部診断 LED（7 ページ）

Cisco SNS-3415/3495 アプライアンスの前面パネル ビュー

図 1(3 ページ) に Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの前面パネル ビューのコンポーネントを示します。

表 2(5 ページ) では、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの前面パネルに配置された LED について説明します。

表 2　前面パネルの LED

LED 名	状態
電源ボタン/電源ステータス LED	■ 消灯:サーバに AC 電力が供給されていません。 ■ オレンジ:サーバはスタンバイ電源モードです。CIMC と一部のマザーボード機能にだけ電力が供給されています。 ■ 緑:サーバは主電源モードです。すべてのサーバ コンポーネントに電力が供給されています。
ID	■ 消灯:ID LED は使用されていません。 ■ 青:ID LED がアクティブです。
システム ステータス	■ 緑:サーバは正常動作状態で稼働しています。 ■ 緑の点滅:サーバはシステムの初期化とメモリ チェックを行っています。 ■ オレンジの点灯:サーバは縮退運転状態にあります。次に例を示します。 – 電源装置の冗長性が失われている。 – CPU が一致しない。 – 少なくとも 1 つの CPU に障害が発生している。 – 少なくとも 1 つの DIMM に障害が発生している。 – RAID 構成内の少なくとも 1 台のドライブに障害が発生している。 ■ オレンジの点滅:サーバは重大な障害発生状態にあります。次に例を示します。 – ブートに失敗した。 – 修復不能な CPU またはバス エラーが検出された。 – サーバが過熱状態にある。
ファン ステータス	■ 緑:すべてのファン モジュールが正常に動作中です。 ■ オレンジの点灯:1 つのファン モジュールに障害が発生しています。 ■ オレンジの点滅:重大な障害。2 つ以上のファン モジュールに障害が発生しています。
温度ステータス	■ 緑:サーバは正常温度で稼働中です。 ■ オレンジの点灯:1 つ以上の温度センサーが警告しきい値を超過しています。 ■ オレンジの点滅:1 つ以上の温度センサーが重大しきい値を超過しています。
電源ステータス	■ 緑:すべての電源装置が正常に動作中です。 ■ オレンジの点灯:1 台以上の電源装置が縮退運転状態にあります。 ■ オレンジの点滅:1 台以上の電源装置が重大な障害発生状態にあります。

表 2　前面パネルの LED（続き）

LED 名	状態
ネットワーク リンク アクティビティ	■ 消灯：イーサネット リンクがアイドル状態です。 ■ 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 ■ 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。
ハード ドライブ障害	■ 消灯：ハード ドライブは正常に動作中です。 ■ オレンジ：このハード ドライブに障害が発生しています。 ■ オレンジの点滅：デバイスの再構成中です。
ハード ドライブ アクティビティ	■ 消灯：ハード ドライブ スレッドにハード ドライブが存在しません（アクセスなし、障害なし）。 ■ 緑：ハード ドライブの準備が完了しています。 ■ 緑の点滅：ハード ドライブはデータの読み取り中または書き込み中です。

Cisco SNS-3415/3495 アプライアンスの背面パネル ビュー

図 2（3 ページ） に Cisco SNS-3415 アプライアンスおよび Cisco 3495 アプライアンスの背面パネル ビューのコンポーネントを示します。

表 3（6 ページ） では、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの前面パネルに配置された LED について説明します。

表 3　背面パネルの LED

LED 名	状態
電源装置障害	■ 消灯：電源装置は正常に動作中です。 ■ オレンジの点滅：イベント警告しきい値に達しましたが、電源装置は動作し続けています。 ■ オレンジの点灯：重大障害しきい値に達し、電源装置がシャットダウンしています（たとえば、ファンの障害や過熱状態など）。
電源装置 AC OK	■ 消灯：電源装置に AC 電力が供給されていません。 ■ 緑の点滅：AC 電力の供給は OK、DC 出力は使用できません。 ■ 緑の点灯：AC 電力供給も、DC 出力も OK。
1 GbE イーサネット専用管理リンク速度	■ 消灯：リンク速度は 10 Mbps です。 ■ オレンジ：リンク速度は 100 Mbps です。 ■ 緑：リンク速度は 1 Gbps です。
1-GbE イーサネット専用管理リンク ステータス	■ 消灯：リンクが確立されていません。 ■ 緑：リンクはアクティブです。 ■ 緑の点滅：アクティブなリンクにトラフィックが存在します。

表 3　背面パネルの LED（続き）

LED 名	状態
1-GbE イーサネット リンク速度	■ 消灯：リンク速度は 10 Mbps です。 ■ オレンジ：リンク速度は 100 Mbps です。 ■ 緑：リンク速度は 1 Gbps です。
1-GbE イーサネット リンク ステータス	■ 消灯：リンクが確立されていません。 ■ 緑：リンクはアクティブです。 ■ 緑の点滅：アクティブなリンクにトラフィックが存在します。
ID	■ 消灯：ID LED は使用されていません。 ■ 青：ID LED がアクティブです。

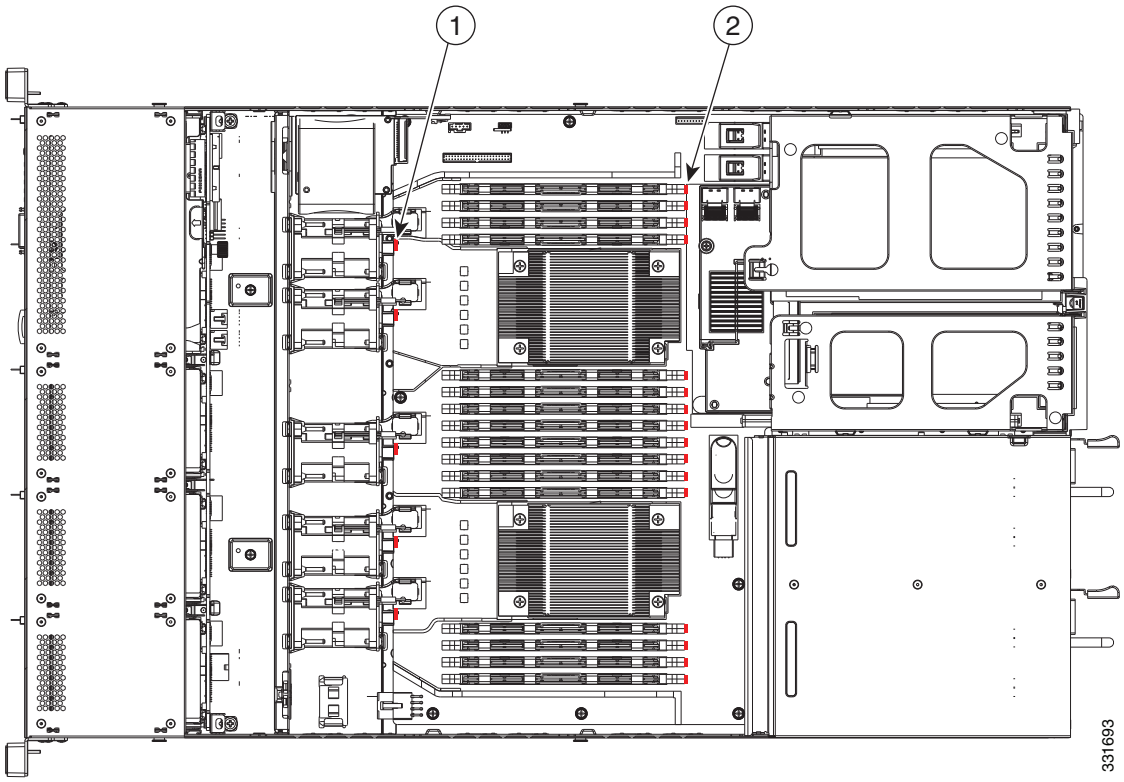
内部診断 LED

サーバには、ファン モジュールと DIMM の内部障害 LED があります。障害が発生しているコンポーネントの LED がオレンジに点灯します。

注：これらの LED が動作するには、サーバに電源が接続されている必要があります。

図 3（7 ページ） に Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの内部 LED の位置を示します。

図 3　Cisco SNS-3415 の内部診断 LED の位置



次の表で、図 3（7 ページ）の各コンポーネントについて説明します。

1	ファン モジュール障害 LED（マザーボード上の各ファン コネクタの隣に 1 個）	2	DIMM 障害 LED（マザーボード上の各 DIMM ソケットの隣に 1 つ）

表 4（8 ページ）では、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスに搭載された内部診断 LED について説明します。

表 4　内部診断 LED

LED 名	状態
内部診断 LED（すべて）	■ 消灯：コンポーネントは正常に機能しています。 ■ オレンジ：コンポーネントに障害が発生しています。

法規制の遵守

法令準拠および安全性に関する情報については、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を参照してください。

詳細については、マニュアルの入手方法およびテクニカル サポート（11 ページ）を参照してください。

Cisco SNS 3415 および Cisco SNS 3495 ハードウェア アプライアンスの設置の準備

ここでは、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスを安全に設置するために場所を準備する方法について説明します。

ここでは、次の項目について説明します。

- 安全に関する注意事項（1 ページ）
- サーバの開梱と点検（2 ページ）
- サーバの設置準備（3 ページ）
- サーバの仕様（4 ページ）

安全に関する注意事項

注：Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの設置、操作、または保守を行う前に、安全上の重要事項について、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を確認します。

警告：**安全上の重要事項**

「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。
ステートメント 1071

警告：**システムの過熱を防ぐため、最大推奨周囲温度の 40°C（104°F）を超えるエリアで操作しないでください。**
ステートメント 1047

警告：**いつでも装置の電源を切断できるように、プラグおよびソケットにすぐに手が届く状態にしておいてください。**
ステートメント 1019

警告：**この製品は、設置する建物に短絡（過電流）保護機構が備わっていることを前提に設計されています。この保護装置の定格が 250 V、15 A 以下であることを確認します。**
ステートメント 1005

警告：**装置は地域および国の電気規則に従って設置する必要があります。**
ステートメント 1074

サーバを設置する際には、次のガイドラインに従ってください。

- サーバを設置する前に、設置場所の構成を計画し、設置環境を整えます。設置場所を計画する際に推奨される作業については、『*Cisco UCS Site Preparation Guide*』を参照してください。
- サーバの周囲に、保守作業および適切な通気のための十分なスペースがあることを確認します。サーバ内では前面から背面へ空気が流れます。

- 空調が、サーバの仕様（4 ページ）に記載された温度要件に適合していることを確認します。
- キャビネットまたはラックが、ラックに関する要件（3 ページ）に記載された要件に適合していることを確認します。
- 設置場所の電源が、サーバの仕様（4 ページ）に記載された電源要件に適合していることを確認します。使用可能な場合は、電源障害に備えて無停電電源装置（UPS）を使用してください。

注意：鉄共振技術を使用する UPS タイプは使用しないでください。このタイプの UPS は、Cisco UCS などのシステムに使用すると、データ トラフィック パターンの変化によって入力電流が大きく変動し、動作が不安定になるおそれがあります。

サーバの開梱と点検

注意：サーバの内部コンポーネントを取り扱うときは ESD ストラップを使用し、モジュールは端の部分を持ってください。

注：サーバの輸送が必要となる場合に備えて、輸送用の箱は保管しておいてください。

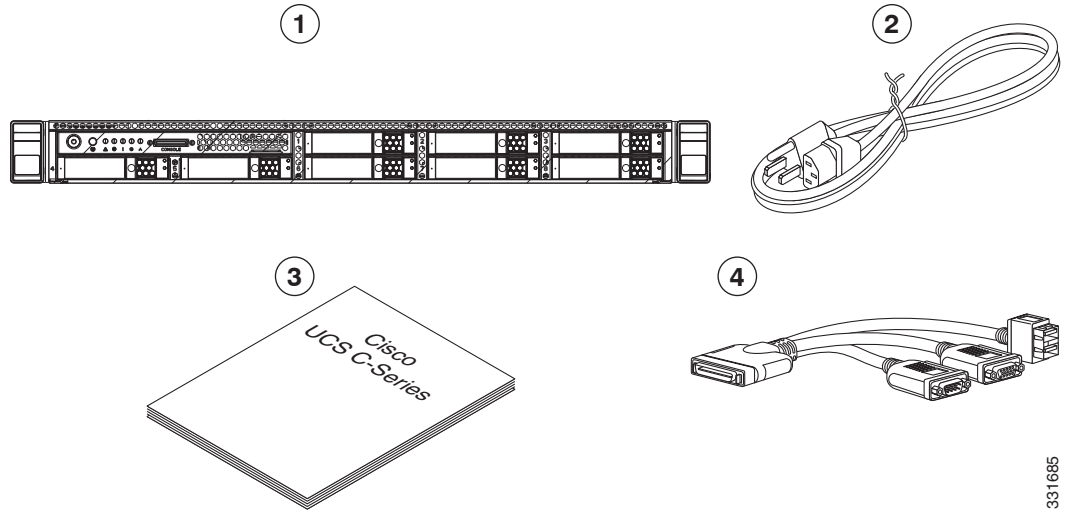
注：シャーシは厳密に検査したうえで出荷されています。輸送中の破損や内容品の不足がある場合には、ただちにカスタマー サービス担当者に連絡してください。

梱包内容を確認する手順は、次のとおりです。

1. 段ボール箱からサーバを取り出します。梱包材はすべて保管しておいてください。
2. カスタマー サービス担当者から提供された機器リストおよび図 1（2 ページ）と、梱包品の内容を照合します。すべての品目が揃っていることを確認してください。
3. 破損の有無を調べ、内容品の間違いや破損がある場合には、カスタマー サービス担当者に連絡してください。次の情報を用意しておきます。

- 発送元の請求書番号（梱包明細を参照）
- 破損している装置のモデルとシリアル番号
- 破損状態の説明
- 破損による設置への影響

図 1　梱包内容



1	サーバ	3	資料
2	電源コード（オプション、最大 2 本）	4	KVM ケーブル

サーバの設置準備

ここでは、サーバの設置準備について説明します。この項の内容は次のとおりです。

- 設置に関するガイドライン（3 ページ）
- ラックに関する要件（3 ページ）
- 機器の要件（4 ページ）
- スライド レールの調整範囲（4 ページ）

設置に関するガイドライン

警告：システムの過熱を防ぐため、最大推奨周囲温度の 40°C（104°F）を超えるエリアで操作しないでください。
ステートメント 1047

警告：いつでも装置の電源を切断できるように、プラグおよびソケットにすぐに手が届く状態にしておいてください。
ステートメント 1019

警告：この製品は、設置する建物に短絡（過電流）保護機構が備わっていることを前提に設計されています。この保護装置の定格が 250 V、15 A 以下であることを確認します。
ステートメント 1005

警告：装置は地域および国の電気規則に従って設置する必要があります。
ステートメント 1074

サーバを設置する際には、次のガイドラインに従ってください。

- サーバを設置する前に、設置場所の構成を計画し、設置環境を整えます。設置場所を計画する際に推奨される作業については、『*Cisco UCS Site Preparation Guide*』を参照してください。
- サーバの周囲に、保守作業および適切な通気のための十分なスペースがあることを確認します。サーバ内では前面から背面へ空気が流れます。
- 空調が、サーバの仕様（4 ページ）に記載された温度要件に適合していることを確認します。
- キャビネットまたはラックが、ラックに関する要件（3 ページ）の項に記載された要件に適合していることを確認します。
- 設置場所の電源が、サーバの仕様（4 ページ）に記載された電源要件に適合していることを確認します。使用可能な場合は、電源障害に備えて無停電電源装置（UPS）を使用してください。

注意：鉄共振技術を使用する UPS タイプは使用しないでください。このタイプの UPS は、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスなどのシステムに使用すると、データ トラフィック パターンの変化によって入力電流が大きく変動し、動作が不安定になることがあります。

ラックに関する要件

ここでは、標準的なオープン ラックの要件について説明します。

次のタイプのラックを使用する必要があります。

- 標準的な 48.3 cm（19 インチ）幅 4 支柱 EIA ラック（ANSI/EIA-310-D-1992 のセクション 1 に準拠した英国ユニバーサル ピッチに適合するマウント支柱付き）。
- 付属のスライド レールを使用する場合、ラック支柱の穴は、0.38 インチ（9.6 mm）の正方形、0.28 インチ（7.1 mm）の丸形、#12-24 UNC、または #10-32 UNC になります。
- サーバあたりの縦方向の最小ラック スペースは、1 RU、つまり 1.75 インチ（44.45 mm）である必要があります。

機器の要件

このサーバ用にシスコから提供されるスライド レールの場合、取り付けに必要な工具はありません。内側のレール（取り付けブラケット）が、サーバの側面にあらかじめ取り付けられています。

スライド レールの調整範囲

このサーバのスライド レールの調整範囲は 24 ～ 36 インチ（610 ～ 914 mm）です。

サーバの仕様

ここでは、サーバの技術仕様について説明します。内容は次のとおりです。

- 物理的仕様（4 ページ）
- 環境仕様（4 ページ）
- 電源仕様（5 ページ）

物理的仕様

表 1（4 ページ）に、サーバの物理的仕様を示します。

表 1　物理的仕様

説明	仕様
高さ	4.3 cm（1.7 インチ）
幅	42.9 cm（16.9 インチ）
奥行き	72.4 cm（28.5 インチ）
重量（フル装備のシャーシ）	16.1 Kg（35.6 ポンド）

環境仕様

表 2（4 ページ）に、サーバの環境仕様を示します。

表 2　環境仕様

説明	仕様
動作時温度	41 ～ 104°F（5 ～ 40°C） 海抜 305 m ごとに最高温度が 1°C 低下。
非動作時温度	-40 ～ 149°F（-40 ～ 65°C）
湿度（RH）、結露なし	10 ～ 90 %
動作時高度	0 ～ 3,048 m（0 ～ 10,000 フィート）
非動作時高度	0 ～ 12,192 m（0 ～ 40,000 フィート）
音響出力レベル ISO7779 に基づく A 特性音響出力レベル LwAd（Bels）を測定 23 °C（73 °F）で動作	5.4

表 2　環境仕様（続き）

説明	仕様
騒音レベル ISO7779 に基づく A 特性音圧レベル LpAm（dBA）を測定 23 °C（73 °F）で動作	37

電源仕様

2 つの電源オプションの電源仕様を次に示します。

- 450 W 電源（5 ページ）
- 650 W 電源（6 ページ）

次の URL にある Cisco UCS Power Calculator を使用すると、ご使用のサーバ設定の電源に関する詳細情報を取得できます。

http://www.cisco.com/assets/cdc_content_elements/flash/dataCenter/cisco_ucs_power_calculator/

注：サーバに異なる種類の電源を混在させないでください。電源装置は、両方とも 450 W、あるいは 650 W にする必要があります。

注：ACS 5.8.1 は、Cisco SNS-3415-K9 のオプションの冗長電源装置をサポートします。

450 W 電源

表 3（5 ページ）に、サーバの環境仕様を示します。

表 3　電源ユニットの仕様

説明	仕様
AC 入力電圧範囲	低範囲：100 ～ 120 VAC 高範囲：200 ～ 240 VAC
AC 入力周波数	範囲：47 ～ 63 Hz（単相、公称 50 ～ 60Hz）
AC 回線入力電流（定常ステート）	6.0 A（100 VAC で最大） 3.0 A（208 VAC で最大）
各電源装置の最大出力電力	450 W
電源装置の出力電圧	主電源：12 VDC スタンバイ電源：12 VDC

650 W 電源

表 4（6 ページ）に、サーバの環境仕様を示します。

表 4　電源ユニットの仕様

説明	仕様
AC 入力電圧範囲	90 ～ 264 VAC（自己調整、公称 180 ～ 264 VAC）
AC 入力周波数	範囲：47 ～ 63 Hz（単相、公称 50 ～ 60Hz）
AC 回線入力電流（定常ステート）	7.6 A（100 VAC で最大） 3.65 A（208 VAC で最大）
各電源装置の最大出力電力	650 W
電源装置の出力電圧	主電源：12 VDC スタンバイ電源：12 VDC

Cisco SNS 3415 および Cisco SNS 3495 ハードウェア アプライアンスの設置

この章では、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの設置方法とネットワークへの接続方法について説明します。

内容は、次のとおりです。

- Cisco SNS-3415/3495 アプライアンス ラックの設置（1 ページ）
- Cisco Integrated Management Controller（CIMC）（4 ページ）
- CIMC の設定（5 ページ）
- ケーブルの接続（7 ページ）
- Cisco SNS-3415/3495 アプライアンスの接続と電源投入（10 ページ）

設置を始める前に、『*Regulatory Compliance and Safety Information for the Cisco 3415 or 3495 Secure Access Control System*』を参照してください。

警告：この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。ステートメント 1030

警告：この装置は、立ち入りが制限された場所への設置を前提としています。立ち入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段を使用しないと入室できない場所を意味します。
ステートメント 1017

Cisco SNS-3415/3495 アプライアンス ラックの設置

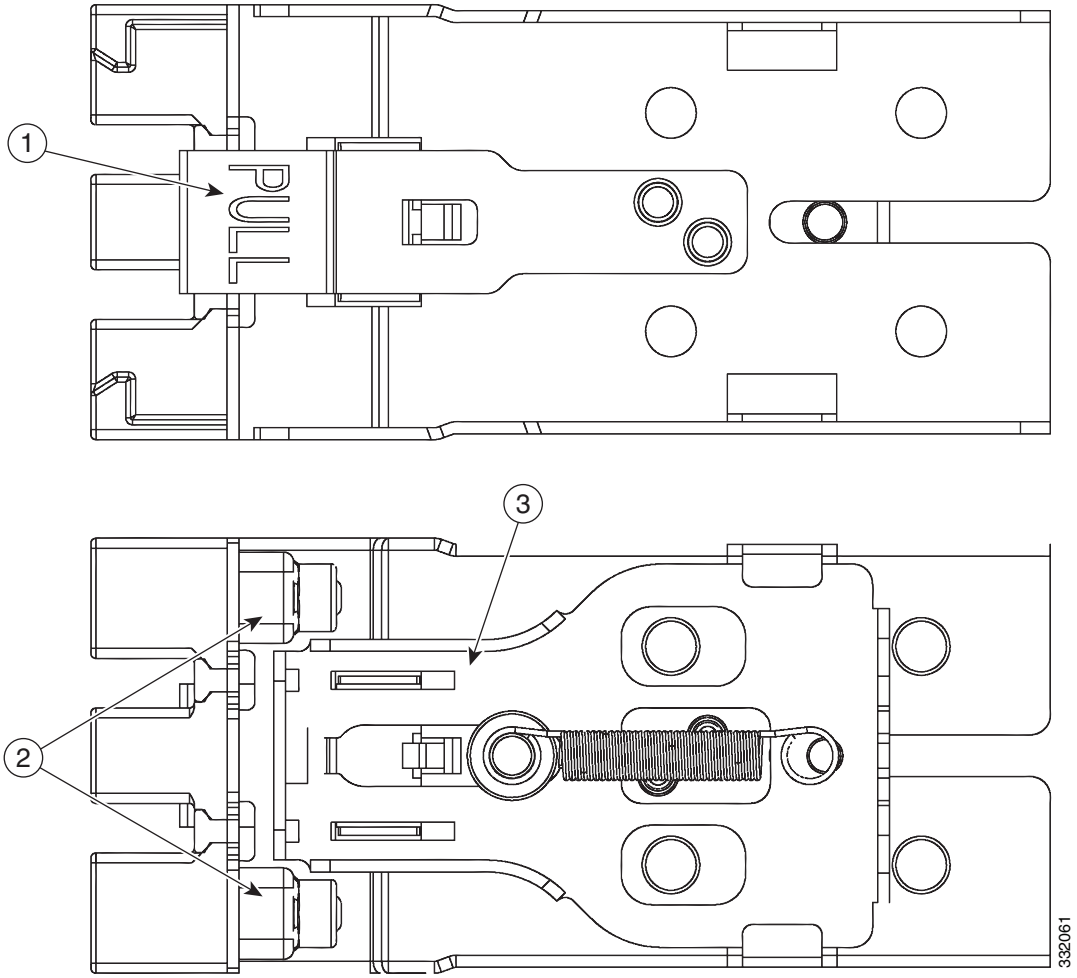
ここでは、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスをラックに設置する方法について説明します。

警告：ラックへのユニットの設置や、ラック内のユニットの保守作業を行う場合は、負傷事故を防ぐため、システムが安定した状態で置かれていることを十分に確認してください。安全を確保するために、次の注意事項を守ってください。
ラックに設置する装置が 1 台だけの場合は、ラックの一番下に取り付けます。
ラックにすでに他の装置が搭載されている場合は、最も重いコンポーネントをラックの一番下にして、重い順に下から上へと搭載するようにしてください。
ラックにスタビライザが付いている場合は、スタビライザを取り付けてから、ラックに装置を設置したり、ラック内の装置を保守したりしてください。
ステートメント 1006

スライド レールとサーバをラックに取り付けるには、次の手順に従います。

1. 前面側の固定ラッチを開きます（図 1（2 ページ） を参照）。スライド レール部品の「FRONT」のマークの付いた端部に、バネ仕掛けの固定ラッチがあります。取り付けペグをラック支柱の穴に挿入する前に、この固定ラッチが開いている必要があります。
   a. 固定ラッチ部品の背面側で、「PULL」のマークの付いたクリップを開いた状態に維持します。
   b. バネ仕掛けの固定ラッチを取り付けペグから離れる方向にスライドさせます。
   c. 開位置で「PULL」クリップを解放して固定ラッチをロックします。

図 1　前面側の固定ラッチ



1	部品の背面にある「PULL」のマークの付いたクリップ	3	部品の前面にあるバネ仕掛けの固定ラッチ
2	前面側の取り付けペグ		

2. 次の手順に従って、スライド レールをラックに取り付けます。

   a. 左側の 2 本のラック支柱の内側でスライド レール部品の位置を合わせます（図 2（3 ページ） を参照）。

   スライド レール部品上の「FRONT」および「REAR」のマークを使用して、ラックの前後の支柱の向きに部品を正しく合わせます。

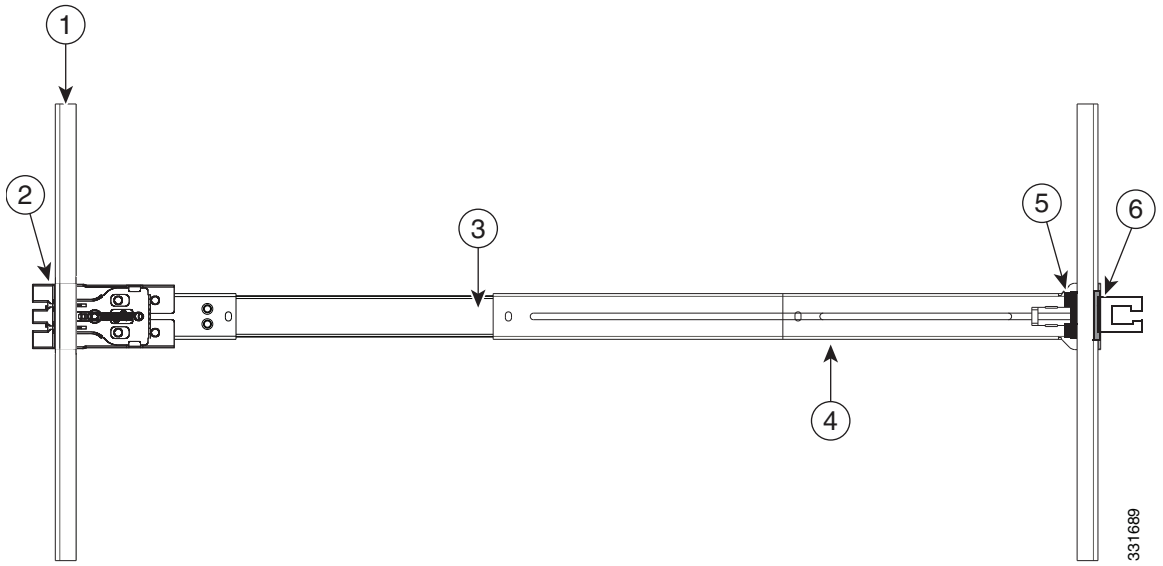
   b. 前面側のラック支柱の目的の穴に前面から入るように、前面側の取り付けペグの位置を合わせます。

   注：ラック支柱の穴を通る取り付けペグは、丸形または正方形の穴か、より小さい #10-32 の丸形の穴（取り付けペグの圧縮時）に適合するように設計されています。ラックに #10-32 のラック支柱の穴がある場合は、取り付けペグをそれらの穴の位置に合わせてから、バネ仕掛けのペグを圧縮して内側の #10-32 ベグを露出させます。

   c. 取り付けペグがラックの後側の支柱の目的の穴にはまるまで、長さ調整ブラケットを伸ばします。

   穴に背面側の取り付けペグを挿入する際、背面の固定ラッチを指で開いたままにします。ラッチを放すと、ラックの支柱が巻き込まれ、スライド レール部品が固定されます。

図 2　スライド レール部品の取り付け



1	左前側ラック支柱	4	長さ調整ブラケット
2	前面側の取り付けペグ	5	背面側の取り付けペグ
3	スライド レール部品	6	背面側の固定ラッチ

d. 2 つ目のスライド レール部品を、ラックの反対側に取り付けます。2 つのスライド レール部品が水平で同じ高さになっていることを確かめます。

e. 所定の位置に収まって留まるまで、各部品の内側のスライド レールをラック前方へ引き出します。

3. サーバを次のようにスライド レールに装着します。

注:内側のレールは、工場出荷時にサーバの側面にあらかじめ取り付けられています。内側のレールが損傷したり、失われたりした場合は、交換用の内側レールを発注できます(Cisco PID UCSC-RAIL1-I)。

a. サーバ側面にある内側レールを、空のスライド レールの前側に合わせます。

b. 内部の停止位置に収まるまで、サーバをスライド レールに押し込みます。

c. プラスチック製の解除クリップ(「PUSH」のラベルのついた)を内側の各レールに押し込み、次に、全面側のラッチがラック支柱に差し込まれるまでサーバをラックに押し込みます。

4. (オプションの)ケーブル マネジメント アーム(CMA)をスライド レールの後ろ側に取り付けます。

注:CMA は左右どちらのレールにも取り付けられるようになっています。次の手順では、サーバの背面から見て、右側のスライド レールの後部に取り付ける方法について説明します。

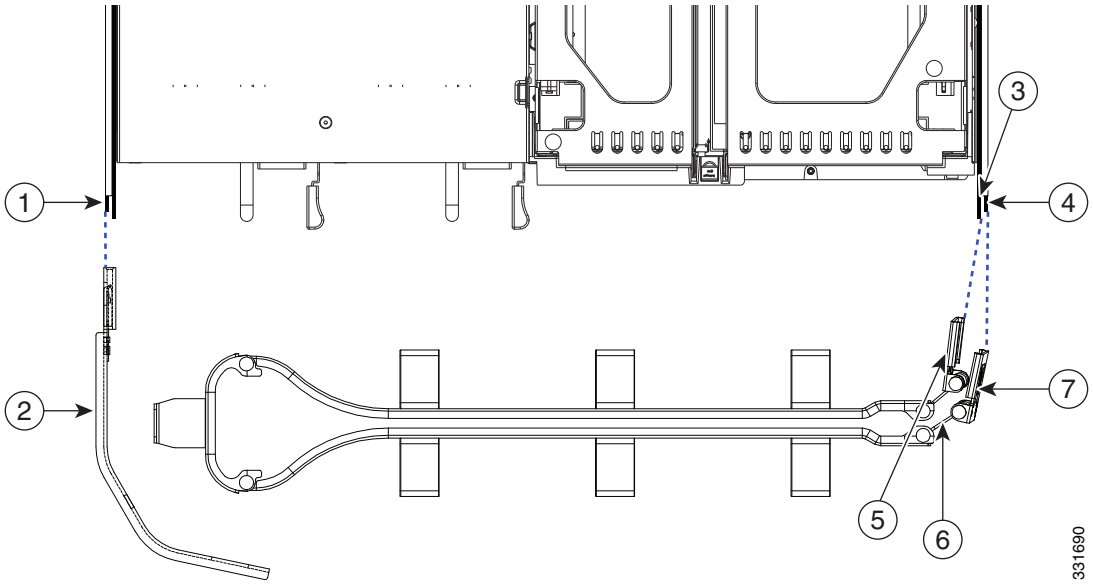
a. 内側の CMA アーム上のプラスチック製クリップを、サーバの側面にある取り付けブラケットのフランジ上でスライドさせます。図 3(4 ページ)を参照してください。

注:CMA を取り付けるスライド レールが左右どちらにあるかに関係なく、必ず「UP」のマークが CMA の上側になるように注意してください。図 3(4 ページ)を参照してください。

b. 外側の CMA アーム上のプラスチック製クリップを、スライド レールのフランジ上でスライドさせます。図 3（4 ページ）を参照してください。

c. CMA 固定ブラケットを左側のスライド レールに取り付けます。ブラケット上のプラスチック製クリップを、左側のスライドの端部にあるフランジ上でスライドさせます。

図 3　ケーブル マネジメント アームの取り付け（サーバの後部）



1	外側の左側スライド レールの後部にあるフランジ	5	内側 CMA アームの取り付けクリップ
2	CMA 固定ブラケット	6	「UP」の方向マーク
3	右側の取り付けブラケットの後部にあるフランジ	7	外側 CMA アームの取り付けクリップ
4	外側の右側スライド レールの後部にあるフランジ	8	

5. 「Cisco SNS-3415/3495 アプライアンスの接続と電源投入」に進みます。

Cisco Integrated Management Controller（CIMC）

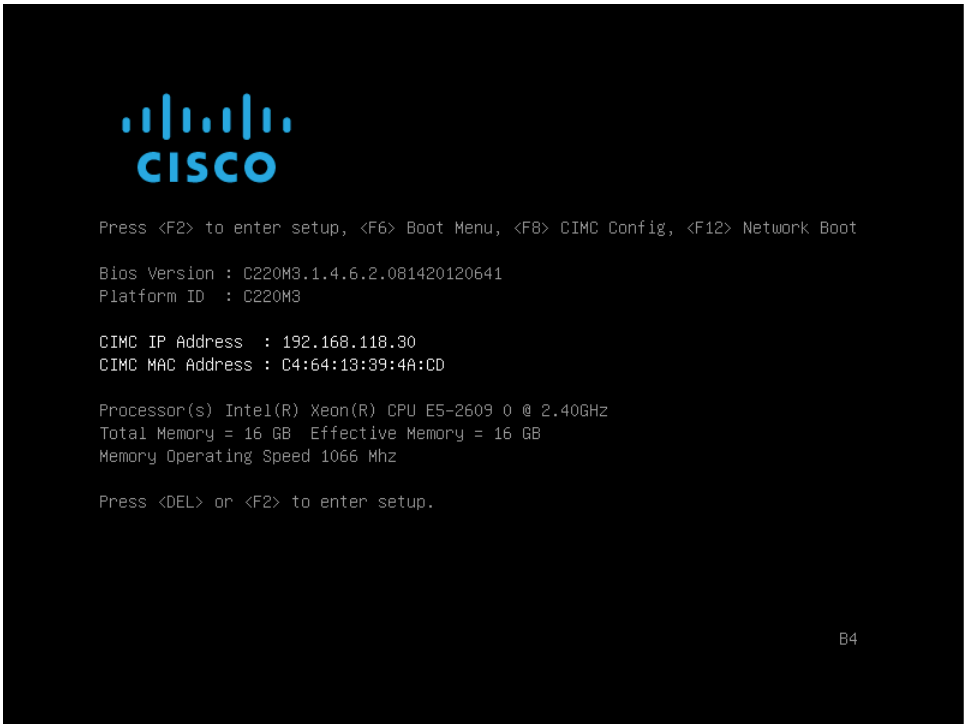
組み込みの Cisco Integrated Management Controller 1.4.7a（CIMC）GUI または CLI インターフェイスを使用して、サーバ インベントリ、状態、およびシステム イベント ログをモニタできます。次の URL で、使用しているファームウェア リリースのユーザ マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

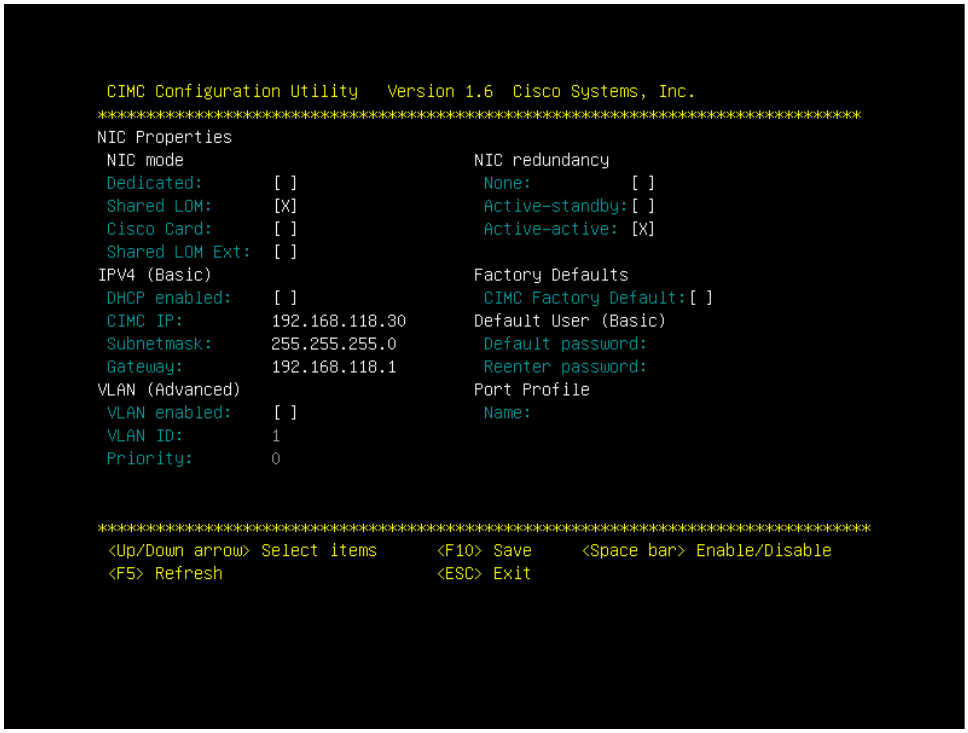
CIMC の設定

CIMC を通じて、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスに対するすべての操作を実行できます。これを行うには、最初に Web ベースのブラウザから CIMC にアクセスするための IP アドレスと IP ゲートウェイを設定する必要があります。

1. 電源コードを差し込みます。
2. 電源ボタンを押して、サーバをブートします。



3. ブートアップ時に、F8 を押して BIOS CIMC 設定ユーティリティを開きます。次の画面が表示されます。



4. サーバ管理用の CIMC へのアクセスに使用するために選択したポートに応じて NIC モードを設定します（ポートの識別については、図 1（3 ページ）を参照してください）。

   - [Dedicated]：CIMC へのアクセスに 1 Gb イーサネット管理ポートを使用します。[NIC redundancy] の[None] を選択し、各種 IP 設定を選択する必要があります。
   - [Shared LOM]（デフォルト）：CIMC へのアクセスに 2 個の 1 Gb イーサネット ポートを使用します。これは工場出荷時設定で、NIC 冗長化は Active-active、DHCP はイネーブルに設定されています。
   - [Cisco Card]：CIMC へのアクセス用に取り付けられている Cisco UCS P81E VIC のポートを使用します。NIC 冗長化と IP 設定を選択する必要があります。

   注：現在、Cisco Card NIC モードは PCIe のスロット 1 に取り付けられている Cisco UCS P81E VIC（N2XX-ACPCI01）のみに対応しています。

5. 必要に応じて NIC 冗長化を変更するには、このユーティリティを使用します。このサーバでは、次の 3 つの NIC 冗長化設定を行うことができます。

   - [None]：イーサネット ポートは個別に動作し、問題が発生した場合にフェールオーバーを行いません。
   - [Active-standby]：アクティブなイーサネット ポートに障害が発生した場合、スタンバイ ポートにトラフィックがフェールオーバーします。
   - [Active-active]：すべてのイーサネット ポートが同時に使用されます。

6. ダイナミック ネットワーク設定用に DHCP をイネーブルにするか、スタティック ネットワーク設定を入力するかを選択します。

   注：DHCP を有効にする前に、あらかじめ DHCP サーバの MAC アドレスの範囲を設定しておく必要があります。MAC アドレスはサーバ背面のラベルに印字されています。このサーバでは、CIMC に 6 つの MAC アドレスの範囲が割り当てられています。ラベルに印字されている MAC アドレスは、6 つの連続 MAC アドレスのうち最初のものです。

7. 任意：このユーティリティを使用して、VLAN 設定を行います。

8. このユーティリティを使用して、デフォルトの CIMC ユーザ パスワードの設定を行います。

   注: 設定の変更は 45 秒ほどで有効になります。次の手順のサーバの再起動は、F5 を押して更新し、新しい設定が表示されてから行います。

9. F10 を押して設定を保存し、サーバをリブートします。

   注: DHCP を有効にすると、ブートアップの間、動的に割り当てられた IP アドレスと MAC アドレスがコンソール画面に表示されます。

注: デフォルトでは、シリアル ポートのボー レートは 115200 に設定されます。CIMC を設定したら、CIMC ユーザ インターフェイスにログインし、シリアル ポートのボー レートを 9600 に変更します。

ケーブルの接続

ここでは、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスをネットワークおよびアプライアンス コンソールに接続する方法について説明します。この項では、次の内容について説明します。

- ネットワーク インターフェイスの接続（7 ページ）
- コンソールの接続（8 ページ）
- キーボードとビデオ モニタの接続（9 ページ）
- ケーブル管理（9 ページ）

ケーブル（必要に応じてキーボード、モニタ ケーブルなど）をサーバの背面に接続します。ケーブルを適切に通し、ケーブル ストラップを使用して、ケーブルをしっかりスライド レールに固定します。アプライアンスの背面図については、図 2（3 ページ）図 2Cisco SNS-3415/3495 アプライアンスの背面図（3 ページ）を参照してください。

ネットワーク インターフェイスの接続

警告: 雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

ここでは、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスのイーサネット ポートを接続する方法について説明します。

イーサネット コネクタは、Serial over LAN（SoL）ケーブルをサポートしています。RJ-45 ポートは、標準的なストレートおよびクロス カテゴリ 5 Unshielded Twisted-Pair（UTP）ケーブルをサポートしています。シスコではカテゴリ 5 UTP ケーブルを販売していません。市販のケーブルを使用してください。

ケーブルをアプライアンスのイーサネット ポートに接続するには、次の手順を実行します。

1. アプライアンスの電源がオフになっていることを確認します。
2. ケーブルの一方の端を、アプライアンス上の GigabitEthernet 0 ポートに接続します。
3. 他方の端をネットワークのスイッチに接続します。

イーサネット ポート コネクタ

Cisco SNS 3415 または Cisco SNS-3495 アプライアンスには、2 個の内蔵デュアルポート イーサネット コントローラが搭載されています。ACS 5.8.1 は複数の NIC をサポートしています。詳細については、複数のネットワーク インターフェイス コネクタ（9 ページ）を参照してください。これらのコントローラでは 10-Mb/s、100-Mb/s、または 1000-Mb/s ネットワークに接続するためのインターフェイスと全二重（FDX）機能が提供され、イーサネット LAN 上でデータを同時に送受信できます。

イーサネット ポートにアクセスするには、カテゴリ 3、4、5、5E、または 6 のシールドなしツイストペア（UTP）ケーブルを、アプライアンスの背面にある RJ-45 コネクタに接続します。

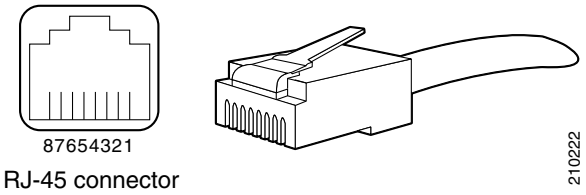
表 1（8 ページ）に、UTP ケーブルのカテゴリを示します。

表 1　イーサネット ケーブル接続ガイドライン

タイプ	説明
10BASE-T	EIA カテゴリ 3、4、または 5 UTP（2 または 4 ペア）、最大 328 フィート（100 m）
100BASE-TX	EIA カテゴリ 5 UTP（2 ペア）、最大 328 フィート（100 m）
1000BASE-T	EIA カテゴリ 6 UTP（推奨）、カテゴリ 5E UTP または 5 UTP（2 ペア）、最大 328 フィート（100 m）

図 4（8 ページ）に、イーサネット RJ-45 ポートとプラグを示します。

図 4　RJ-45 ポートとプラグ



RJ-45 connector

表 2（8 ページ）の一覧では、コネクタで使用される RJ-45 ピン信号について説明します。

表 2　イーサネット ポートのピン配列

イーサネット ポートのピン	信号	説明
1	TxD+	送信データ +
2	TxD-	送信データ -
3	RxD+	受信データ +
4	終端ネットワーク	接続なし
5	終端ネットワーク	接続なし
6	RxD-	受信データ -
7	終端ネットワーク	接続なし
8	終端ネットワーク	接続なし

コンソールの接続

警告：雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

Cisco SNS-3415 または Cisco SNS-3495 アプライアンスには、コンソール端末をアプライアンスに接続するための DCE モードのコンソール ポートがあります。アプライアンスのコンソール ポートでは、DB-9 シリアル コネクタが使用されています。

Cisco SNS-3415 または Cisco SNS-3495 アプライアンス上のコンソール ポートには、EIA/TIA-232 非同期シリアル（DB-9）コネクタが含まれています。このシリアル コンソール コネクタ（ポート）を使用することで、端末（ターミナル エミュレーション ソフトウェアが動作する PC か ASCII 端末）をコンソール ポートに接続し、アプライアンスにローカルにアクセスできます。

ターミナル エミュレーション ソフトウェアが動作する PC をコンソール ポートに接続するには、両端が DB-9 メスのストレート ケーブルを使用します。

ASCII 端末をコンソール ポートに接続するには、片方が DB-9 メスでもう一方が DB-25 オスのストレート ケーブルと、DB-25 メスから DB-25 メスへの変換アダプタを使用します。

端末またはターミナル エミュレーション ソフトウェアが動作する PC を、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスのコンソール ポートに接続するには、次の手順を実行します。

1. ストレート ケーブルを使用して端末をコンソール ポートに接続します。
2. 端末またはターミナル エミュレーション ソフトウェアを、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、ハードウェア フロー制御なしに設定します。

キーボードとビデオ モニタの接続

警告：雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

ここでは、キーボードとビデオ モニタを Cisco SNS-3415 または Cisco SNS-3495 アプライアンスに接続するための方法について説明します。

Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの前面パネルにある KVM コネクタを使用して、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスにキーボードとビデオ モニタを接続できます。KVM ケーブルは、2 個の USB、1 個の VGA、および 1 個のシリアル コネクタを装備するアプライアンスに同梱されています。

Cisco SNS-3415 または Cisco SNS-3495 アプライアンスはマウスをサポートしていません。

Cisco SNS-3415 または Cisco SNS-3495 には、アプライアンスの背面に USB ポートがあり、キーボードとビデオ モニタを接続するために使用できます。

キーボードとビデオ モニタをアプライアンスに接続するには、次の手順を実行します。

1. アプライアンスの電源がオフになっていることを確認します。
2. キーボード ケーブルの端を、アプライアンスの背面パネルにある PS/2（キーボード）ポートに接続します。
3. ビデオ モニタ ケーブルの端を、アプライアンスの背面パネルにある PS/2（ビデオ モニタ）ポートに接続します。
4. アプライアンスの電源をオンにします。

ケーブル管理

ケーブル管理は、アプライアンスの設定の中で、最も外観に関係する作業です。しかし、ケーブル管理には時間がかかるため、放置しがちです。

今日の装置ラックは、従来よりも多くの装置を収納するようになっています。このため、ラックの内部と外部で整然としたケーブル管理を行う必要性が高まっています。ケーブル管理が適切でないと、ケーブルが損傷したりケーブルの追加や変更に時間がかかったりするだけでなく、重要な通気やアクセスが妨げられます。これらの問題により、装置のパフォーマンスが低下したり、ダウンタイムが長くなったりするおそれがあります。

ケーブル管理を扱うためのソリューションは多数あります。単純なケーブル管理リングから、垂直または水平収納容器、樋やはしごに至るまで、さまざまなソリューションがあります。

すべての Cisco SNS-3415 または Cisco SNS-3495 アプライアンス ケーブルは、ケーブル同士や装置の他の部分と干渉しないように、適切に整理する必要があります。各地の慣習に従って、アプライアンスに接続されているケーブルを適切に整理してください。

設置手順を続行するには、次のセクションCisco SNS-3415/3495 アプライアンスの接続と電源投入（10 ページ）に進んでください。

Cisco SNS-3415/3495 アプライアンスの接続と電源投入

- サーバの接続と電源投入（スタンドアロン モード）（10 ページ）
- システム BIOS および CIMC ファームウェア（11 ページ）
- サービス ヘッダーおよびジャンパ（12 ページ）

サーバの接続と電源投入（スタンドアロン モード）

注: このセクションではサーバの電源投入の方法、IP アドレスの割り当て方法、サーバをスタンドアロン モードで使用する場合のサーバ管理への接続方法について説明します。サーバを UCS 統合で使用する場合は、特定のケーブル接続および設定が必要です。『Installation for Cisco UCS Integration』を参照してください。

注: このサーバにはあらかじめ Shared LOM というデフォルトの NIC モードが設定されています。デフォルトの NIC 冗長化はアクティブ-アクティブで、DHCP は有効化されています。[共有 LOM（Shared LOM）] モードでは、2 つの 1 Gb イーサネット ポートが Cisco Integrated Management Interface（CIMC）にアクセスできます。1 Gb イーサネット専用管理ポート、または Cisco UCS P81E 仮想インターフェイス カード（VIC）のポートを使用して CIMC にアクセスする場合は、次の手順のステップ 3 の説明に従って、まずサーバに接続して NIC モードを変更する必要があります。このステップでは、NIC 冗長化を変更し、スタティック IP 設定を設定することもできます。

サーバの初期設定を実行する手順は、次のとおりです。

1. 付属の電源コードをサーバの各電源装置に接続し、次に、接地された AC 電源出力に接続します。電源仕様については、電源仕様（5 ページ）を参照してください。最初のブートアップ中、サーバがスタンバイ電源でブートするまでに約 2 分かかります。

   電源ステータスは、電源ステータス LED で確認できます（参照）。

- 消灯：サーバには AC 電力が供給されていません。
- オレンジ：サーバはスタンバイ電源モードです。CIMC と一部のマザーボード機能にだけ電力が供給されています。
- 緑：サーバは主電源モードです。すべてのサーバ コンポーネントに電力が供給されています。

注: ブートアップ中、接続されている USB デバイスの数だけビープ音が鳴ります。外部の USB デバイスが取り付けられていない場合でも、仮想フロッピー ドライブ、CD/DVD ドライブ、キーボード、またはマウスなどの各仮想 USB デバイスに対して短いビープ音が鳴ります。BIOS 電源投入時自己診断テスト（POST）時に USB デバイスをホットプラグまたはホットアンプラグした場合、または、BIOS セットアップ ユーティリティや EFI シェルにアクセスしている間にもビープ音が鳴ります。

2. 前面パネルの KVM コネクタに接続されている付属の KVM ケーブルを使用して USB キーボードと VGA モニタを接続します（図 1（3 ページ） を参照）。

注: 代わりに、背面パネルの VGA および USB ポートを使用することもできます。ただし、前面パネルの VGA と背面パネルの VGA は同時に使用できません。1 つの VGA コネクタに接続している場合に、反対側のコネクタにビデオ デバイスを接続すると、最初の VGA コネクタが無効になります。

3. BIOS CIMC Configuration Utility を起動するには、CIMC の設定（5 ページ）を参照してください。このユーティリティを使用して、NIC モードと NIC 冗長化を設定し、DHCP をイネーブルにするか、スタティック ネットワーク設定を設定するかを選択します。

4. サーバ管理用の CIMC に接続します。ステップ 3 で選択したポートを使用して、LAN からサーバにイーサネット ケーブルを接続します。[Active-active] および [Active-passive] の [NIC redundancy] 設定では、2 つのポートに接続する必要があります。
5. ブラウザに CIMC の IP アドレスを入力して、CIMC セットアップ ユーティリティに接続します。CIMC IP アドレスは、ステップ 3 に設定されています（スタティック アドレスまたは DHCP サーバによって割り当てられたアドレス）。

サーバを管理するには、これらのインターフェイスの使用手順について『Cisco UCS C-Series Rack-Mount Server Configuration Guide』または『Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide』を参照してください。これらのマニュアルへのリンクは、次の URL の C シリーズ マニュアル ロードマップ内にあります。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

システム BIOS および CIMC ファームウェア

ここでは、システム BIOS 1.4.7b.0 について説明します。この項の内容は次のとおりです。

- BIOS および CIMC ファームウェアの更新（11 ページ）
- システム BIOS へのアクセス（12 ページ）

BIOS および CIMC ファームウェアの更新

注意：BIOS ファームウェアを更新する際には CIMC ファームウェアも同一のバージョンにアップグレードする必要があります。そうしないと、サーバが起動しません。BIOS と CIMC のファームウェアが一致するまで電源をオフにしないでください。オフにすると、サーバが起動しません。
シスコは、BIOS、CIMC、およびその他のファームウェアを互換性のあるレベルに同時にアップグレードできるよう支援するために、Cisco Host Upgrade Utility を提供しています。

サーバには、シスコが提供し、承認しているファームウェアが使用されています。シスコは、各ファームウェア イメージと共にリリース ノートを提供しています。ファームウェアを更新するには、いくつかの方法があります。

- **ファームウェア レベル 1.2 以降を実行するシステムの場合の推奨方法**：Cisco Host Upgrade Utility を使用して、CIMC 1.4.7a、BIOS 1.4.7b.0、LOM、LSI ストレージ コントローラ、および Cisco UCS P81E VIC ファームウェアを同時に互換性のあるレベルにアップグレードします。

ファームウェア レベルについては、下記のマニュアル ロードマップ リンクにある『*Cisco Host Upgrade Utility Quick Reference Guide*』を参照してください。

> **注**：Cisco Host Upgrade Utility を使用するには、システム ファームウェアがレベル 1.2 以降である必要があります。ファームウェアがレベル 1.2 よりも前のレベルである場合は、次の方法で BIOS および CIMC ファームウェアを個別に更新する必要があります。

- EFI インターフェイスを使用して BIOS をアップグレードするか、Windows または Linux プラットフォームからアップグレードすることができます。『Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide』を参照してください。
- CIMC GUI インターフェイスを使用して CIMC と BIOS のファームウェアをアップグレードできます。『Cisco UCS C-Series Rack-Mount Server Configuration Guide』を参照してください。
- CIMC CLI インターフェイスを使用して CIMC と BIOS のファームウェアをアップグレードできます。『Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide』を参照してください。

上記のマニュアルへのリンクについては、次の URL にあるマニュアル ロードマップを参照してください。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

システム BIOS へのアクセス

サーバの BIOS 設定を変更するには、次の手順に従います。詳しい手順は、BIOS 画面にも表示されます。

1. ブートアップ時にメッセージが表示されたら、F2 キーを押して BIOS セットアップ ユーティリティに切り替えます。

   注:現在の BIOS のバージョンとビルドはユーティリティの [Main] ページに表示されます。

2. 矢印キーを使って、BIOS メニュー ページを選択します。
3. 矢印キーを使って、変更するフィールドを反転表示にします。
4. Enter を押して変更するフィールドを選択し、そのフィールドの値を変更します。
5. [Exit] メニュー画面が表示されるまで右矢印キーを押します。
6. [Exit] メニュー画面の指示に従って変更内容を保存し、セットアップ ユーティリティを終了します(または、F10 を押します)。Esc を押すと、変更内容を保存せずにユーティリティを終了できます。

サービス ヘッダーおよびジャンパ

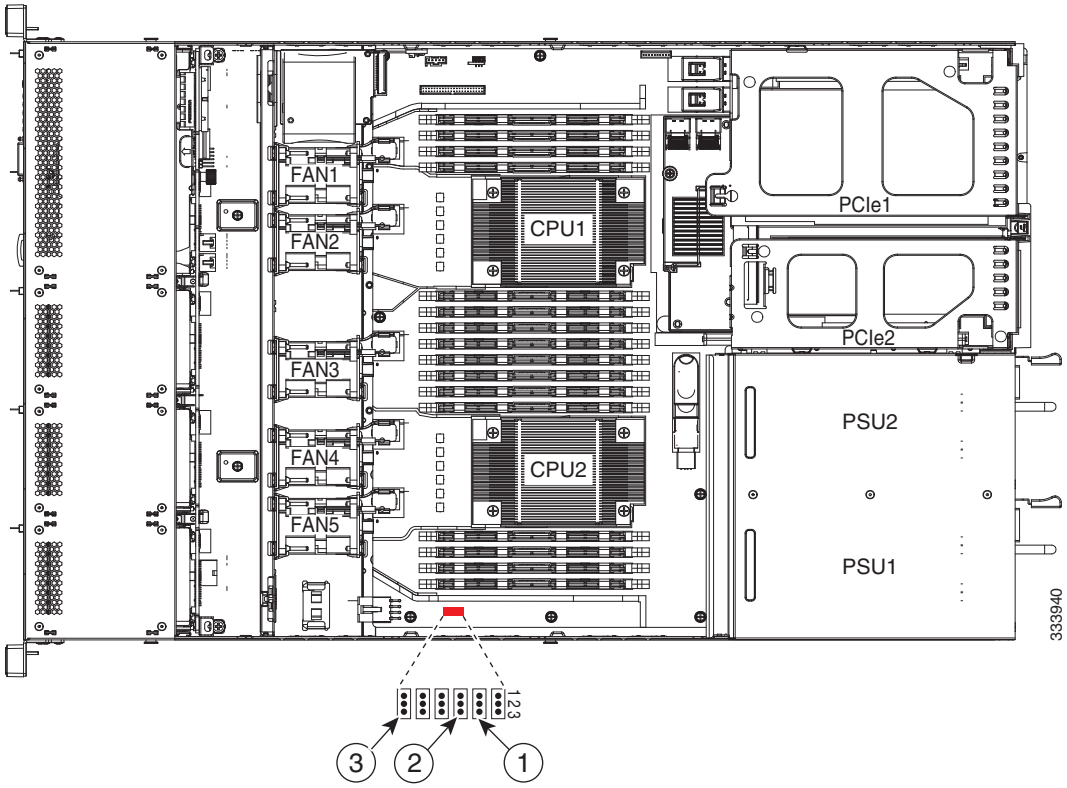
このセクションは、次のトピックで構成されています。

- マザーボードのヘッダーの場所(12 ページ)
- BIOS リカバリ ヘッダー J41 の使用(13 ページ)
- CMOS クリア ヘッダー J37 の使用(15 ページ)

マザーボードのヘッダーの場所

図 5(13 ページ)を参照してください。ヘッダーのブロックが赤色で表示されます。それぞれのヘッダーは拡大ビューに表示されます。ピン番号はブロックのすべてのヘッダーで同じです。

図 5　サービス ヘッダーの場所



1	J41 BIOS RCVR BOOT	2	J37 CMOS のクリア

BIOS リカバリ ヘッダー J41 の使用

BIOS 破損の段階によって、出現する動作が異なります。

- BIOS BootBlock が破損すると、システムが次のメッセージとともに停止する場合があります。

```
Initializing and configuring memory/hardware
```

- BootBlock の破損ではない場合、次のメッセージが表示されます。

```
****BIOS FLASH IMAGE CORRUPTED****
Flash a valid BIOS capsule file using CIMC WebGUI or CLI interface.
IF CIMC INTERFACE IS NOT AVAILABLE, FOLLOW THE STEPS MENTIONED BELOW.
1.Connect the USB stick with recovery.cap file in root folder.
2.Reset the host.
IF THESE STEPS DO NOT RECOVER THE BIOS
1.Power off the system.
2.Mount recovery jumper.
3.Connect the USB stick with recovery.cap file in root folder.
4.Power on the system.
Wait for a few seconds if already plugged in the USB stick.
REFER TO SYSTEM MANUAL FOR ANY ISSUES.
```

注: 上のメッセージの示すように、BIOS 回復には、2 種類の手順があります。手順 1 を試して BIOS が回復しない場合は、手順 2 を使用します。

注: これらの手順を使用するには、サーバの CIMC がバージョンが 1.4(6) 以降でなければなりません。

手順 1：recovery.cap ファイルを使った再起動

1. BIOS 更新パッケージをダウンロードし、一時的な場所に保存して展開します。
2. 展開した [Initializing and configuring memory/hardware] フォルダの内容を USB メモリのルート ディレクトリにコピーします。リカバリ フォルダには、この手順に必要なリカバリ ファイルが含まれます。

   注：recovery.cap ファイルは USB ドライブのルート ディレクトリに存在する必要があります。このファイルの名前を変更しないでください。USB ドライブは、FAT16 または FAT32 ファイル システムでフォーマットする必要があります。
3. USB メモリをサーバの USB ポートに接続します。
4. サーバをリブートします。
5. 前面パネルの**電源**ボタンを押して、サーバを主電源モードに戻します。

   サーバが、更新された BIOS ブート ブロックでブートします。BIOS が USB メモリの有効な recovery.cap ファイルを検出すると、次のメッセージが表示されます。

```
Found a valid recovery file...Transferring to CIMC
System would flash the BIOS image now...
System would restart with recovered image after a few seconds....
```

6. サーバの BIOS 更新が完了するのを待ってから、USB メモリをサーバから取り外します。

   注：BIOS の更新中に、CIMC はサーバをシャット ダウンし、画面には約 10 分間何も表示されません。更新中は、電源コードを外さないでください。更新が完了すると、CIMC はサーバの電源を投入します。

手順 2：リカバリ ジャンパおよび recovery.cap ファイルの使用

J41 ヘッダーの位置については、図 5（13 ページ）を参照してください。

1. BIOS 更新パッケージをダウンロードし、一時的な場所に保存して展開します。
2. 展開したリカバリ フォルダ内のファイルを、USB メモリのルート ディレクトリにコピーします。リカバリ フォルダにはこの手順に必要な recovery.cap ファイルが含まれます。

   注：recovery.cap ファイルは USB ドライブのルート ディレクトリに存在する必要があります。このファイルの名前を変更しないでください。USB ドライブは、FAT16 または FAT32 ファイル システムでフォーマットする必要があります。
3. 「サーバのシャットダウンおよび電源オフ」の説明に従って、サーバの電源をオフにします。
4. 電源装置からすべての電源コードを外します。
5. 上部カバーを取り外せるように、サーバをラックの前方に引き出します。場合によっては、背面パネルからケーブルを取り外して隙間を空ける必要があります。

注意：コンポーネントへの接触や確認作業を安全に行えない場合は、ラックからサーバを取り出してください。

6. 「サーバ上部カバーの取り外しおよび取り付け」の説明に従って、上部カバーを取り外します。
7. J41 ヘッダーのピン 2 および 3 に、ショート ジャンパを移動します（図 2-5 を参照）。
8. AC 電源コードをサーバに再度取り付けます。サーバの電源がスタンバイ電源モードになります。
9. ステップ 2 で準備した USB メモリをサーバの USB ポートに接続します。

10. 前面パネルの電源ボタンを押して、サーバを主電源モードに戻します。

    サーバが、更新された BIOS ブート ブロックでブートします。BIOS が USB メモリの有効な recovery.cap ファイルを検出すると、次のメッセージが表示されます。

    ```
    Found a valid recovery file...Transferring to CIMC
    System would flash the BIOS image now...
    System would restart with recovered image after a few seconds....
    ```

11. サーバの BIOS 更新が完了するのを待ってから、USB メモリをサーバから取り外します。

    注：BIOS の更新中に、CIMC はサーバをシャット ダウンし、画面には約 10 分間何も表示されません。更新中は、電源コードを外さないでください。更新が完了すると、CIMC はサーバの電源を投入します。

12. サーバが完全にブートした後に、サーバの電源を再び切り、すべての電源コードを外します。

13. J41 ヘッダーのデフォルトのピン 1 および 2 に戻るジャンパを移動します。

    注：ジャンパを移動しないと、リカバリ完了後にメッセージ「Please remove the recovery jumper.」が表示されます。

14. 上部カバーを交換し、ラックのサーバを交換し、電源コードおよびその他のケーブルを交換したら、電源ボタンを押してサーバの電源をオンにします。

CMOS クリア ヘッダー J37 の使用

このヘッダーの位置については、図 5（13 ページ） を参照してください。このヘッダーのジャンパで、システムがハング アップしたときにサーバの CMOS 設定をクリアできます。たとえば、設定が正しくないためにサーバがハング アップしてブートしなくなった場合に、このジャンパを使って設定を無効化し、デフォルト設定を使って再起動できます。

注意：CMOS をクリアするとすべてのカスタム設定が消去され、データ損失の原因となることがあります。この CMOS のクリア手順を使用する前に BIOS に必要なカスタマイズされた設定を書き留めます。

1. 「サーバのシャットダウンおよび電源オフ」の説明に従って、サーバの電源をオフにします。
2. 電源装置からすべての電源コードを外します。
3. 上部カバーを取り外せるように、サーバをラックの前方に引き出します。場合によっては、背面パネルからケーブルを取り外して隙間を空ける必要があります。

注意：コンポーネントへの接触や確認作業を安全に行えない場合は、ラックからサーバを取り出してください。

4. 「サーバ上部カバーの取り外しおよび取り付け」の説明に従って、上部カバーを取り外します。
5. J37 ヘッダーのピン 2 および 3 に、ショート ジャンパを移動します（図 2-5 を参照）。
6. 上部カバーと AC 電源コードをもう一度サーバに取り付けます。サーバの電源がスタンバイ電源モードになり、前面パネルの電源 LED がオレンジ色に点灯します。
7. 前面パネルの電源ボタンを押して、サーバを主電源モードに戻します。電源 LED が緑色になれば、サーバは主電源モードです。

   注：リセットを完了するには、修復作業中のプロセッサだけでなく、サーバ全体がリブートして主電源モードになるようにする必要があります。これは、ホスト CPU が実行されていないとジャンパの状態を判別できないからです。

8. 電源ボタンを押し、サーバをシャットダウンしてスタンバイ電源モードにし、電流が流れないようにするために AC 電源コードを抜きます。
9. サーバの上部カバーを外します。

10. ショート ジャンパをヘッダー ピン 2 および 3 からデフォルト位置のピン 1 および 2 に戻します。

    注:ジャンパを移動しないと、サーバの電源を投入するたびに CMOS 設定がデフォルトにリセットされます。

11. 上部カバーを交換し、ラックのサーバを交換し、電源コードおよびその他のケーブルを交換したら、電源ボタンを押してサーバの電源をオンにします。

Cisco SNS-3415 および Cisco SNS-3495 を使用した Secure Access Control System のインストールと設定

この章では、Cisco SNS-3415 または Cisco SNS-3495 と ACS 5.8.1 サーバのインストールおよび初期設定の方法について説明します。

この章の内容は、次のとおりです。

- Cisco SNS-3415/3495 アプライアンスへの ACS のインストール（1 ページ）
- Cisco Secure ACS 5.8.1 ISO イメージのダウンロード（2 ページ）
- ACS サーバのインストール（2 ページ）
- 管理者パスワードのリセット（9 ページ）
- Cisco SNS-3415/3495 アプライアンスのイメージの再作成（10 ページ）

Cisco SNS-3415/3495 アプライアンスへの ACS のインストール

Cisco SNS-3415 または Cisco SNS-3495 アプライアンスには、ACS 5.8.1 ソフトウェアがあらかじめインストールされています。ここでは、インストール プロセスの概要と、ACS をインストールする前に実行する必要がある作業について説明します。

ACS 5.8.1 のインストールを開始する前に、次の作業を実行する必要があります。

1. 箱を開けて内容を確認します。サーバの開梱と点検（2 ページ）を参照してください
2. Cisco SNS-3415 および Cisco SNS-3495 ハードウェア アプライアンスの導入（1 ページ）を参照してください。
3. Cisco SNS 3415 および Cisco SNS 3495 ハードウェア アプライアンスの設置の準備（1 ページ）にある、一般的な注意事項と安全に関する警告を読みます。
4. アプライアンスをラックに取り付けます。サーバの設置準備（3 ページ）を参照してください
5. Cisco SNS-3415 または Cisco SNS-3495 をネットワークとアプライアンス コンソールに接続します。ケーブルの接続（7 ページ）を参照してください
6. Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの電源をオンにします。Cisco SNS-3415/3495 アプライアンスの接続と電源投入（10 ページ）を参照してください
7. ネットワークとアプライアンス コンソールに対して、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの電源をオンにします。ケーブルの接続（7 ページ）を参照してください
8. CLI プロンプトで **setup** コマンドを実行し、ACS サーバの初期設定を行います。セットアップ プログラムの実行（5 ページ）を参照してください。アプライアンス コンソールまたは CIMC を使用して、設定を行うことができます。

『Cisco UCS Server Configuration Utility, Release 3.0 User Guide』ガイドを使用して、Cisco SNS-3415 アプライアンスまたは Cisco SNS-3495 アプライアンスを設定できます。Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの詳細については、『Cisco UCS C-Series Rack Server guides』も参照できます。

Cisco Secure ACS 5.8.1 ISO イメージのダウンロード

Cisco.com から Cisco Secure ACS 5.8.1 ISO イメージをダウンロードできます。

1. http://www.cisco.com/go/acs にアクセスします。このリンクにアクセスするには、有効な Cisco.com ログイン クレデンシャルを所有している必要があります。
2. [Download Software] をクリックします。

Cisco.com ページに Cisco Secure ACS リリース 5.8.1 ソフトウェア イメージが表示されます。インストールおよび初期設定が完了したら、すべての Cisco ACS サービスのテストを実行できます。

注:ACS 5.x ソフトウェア イメージを Cisco.com からダウンロードできるのは、以前のバージョンの ACS 5.x ソフトウェアについて有効な Software Application Support(SAS)契約を結んでいる場合だけです。以前のバージョンで有効な SAS 契約を結んでいない場合は、Cisco.com のソフトウェア イメージを特定のカスタマー アカウントに公開するには、販売エンジニア(SE)、アカウント マネージャ(AM)、またはシスコ パートナーにお問い合わせください。

ACS サーバのインストール

Cisco Secure ACS 5.8.1 ISO イメージをダウンロードしたら、次のいずれかのオプションを使用して、アプライアンスに Cisco Secure ACS 5.8 ソフトウェアをインストールおよび設定できます。

- Cisco Integrated Management Interface(CIMC)を設定し、CIMC を使用して、ネットワークを介してリモートから Cisco Secure ACS 5.8.1 をインストールします。CIMC の設定(5 ページ)、CIMC を使用したリモートからの Cisco SNS-3415/3495 アプライアンスへの ACS 5.8.1 のインストール(2 ページ)、およびセットアップ プログラムの実行(5 ページ)を参照してください。
- ブート可能な USB ドライブを作成し、USB ドライブを使用して、Cisco Secure ACS 5.8.1 をインストールします。ブート可能な USB ドライブの作成(4 ページ)、USB ドライブを使用した Cisco SNS-3415/3495 アプライアンスへの ACS 5.8.1 のインストール(4 ページ)、およびセットアップ プログラムの実行(5 ページ)を参照してください。

CIMC を使用したリモートからの Cisco SNS-3415/3495 アプライアンスへの ACS 5.8.1 のインストール

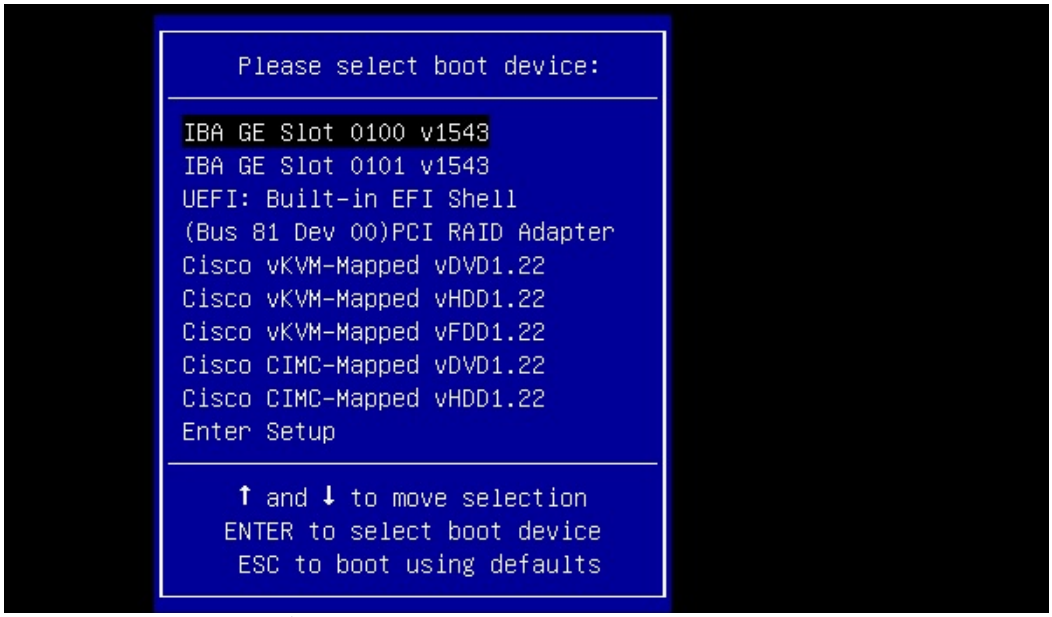
アプライアンスの CIMC を設定したら、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの管理に使用できます。CIMC を通じて、Cisco SNS-3415 または Cisco SNS-3495 アプライアンスで BIOS 設定を含むすべての操作を実行できます。

1. サーバ管理用の CIMC に接続します。NIC モードの設定で選択したポートを使用して、LAN からサーバにイーサネット ケーブルを接続します。[Active-active] および [Active-passive] の [NIC redundancy] 設定では、2 つのポートに接続する必要があります。
2. ブラウザと CIMC の IP アドレスを使用して CIMC セットアップ ユーティリティにログインします。IP アドレスは、設定した CIMC に基づいています(スタティック アドレスまたは DHCP サーバによって割り当てられたアドレス)。

   注:サーバのデフォルトのユーザ名は *admin* です。デフォルト パスワードは *password* です。
3. CIMC クレデンシャルを使用してログインします。
4. [Launch KVM Console] をクリックします。
5. [Virtual Media] をクリックします。
6. 一覧から、[Activate Virtual Devices] を選択します。

   [Activate Virtual Devices] オプション近くのチェックマークが表示されます。
7. [Virtual Media] を再度クリックし、[MAP CD/DVD] オプションを選択します。

8. [Browse] をクリックして ACS 5.8.1 ISO イメージを探します。
9. [Map Device] をクリックします。
10. [Macros] > [Static Macros] > [Ctrl-Alt-Del] の順に選択して、ISO イメージを使用して Cisco SNS-3415 または Cisco SNS-3495 アプライアンスを起動します。
11. F6 キーを押して、ブート メニューを起動します。次のような画面が表示されます。



12. CD/DVD にマッピングした Cisco vKVM-Mapped vDVD を選択して、Enter キーを押します。次のメッセージが表示されます。

```
Welcome to the Cisco Secure ACS 5.8.1 Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS Installation (Keyboard/Monitor)
[2] Cisco Secure ACS Installation (Serial Console)
[3] Recover administrator password (Keyboard/Monitor
[4] Recover administrator password (Serial Console)
<Enter> Boot existing OS from hard disk.
Enter boot option and press <Enter>
boot:
```

13. ブート プロンプトで、1 を入力して、**Enter** キーを押します。
14. セットアップ モードでネットワーク設定パラメータを入力すると、アプライアンスが自動的に再起動し、シェル プロンプト モードに戻ります。
15. シェル プロンプト モードを終了します。アプライアンスが起動します。
16. インストール プロセスの確認（5 ページ）に進みます。

USB ドライブを使用した Cisco SNS-3415/3495 アプライアンスへの ACS 5.8.1 のインストール

USB ドライブを使用して Cisco SNS-3415 または Cisco SNS-3495 アプライアンスに ACS 5.8.1 をインストールするには、次の手順を実行します。

はじめる前に

ブート可能な USB ドライブを作成する必要があります。ブート可能な USB ドライブの作成（4 ページ）を参照してください。

1. Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの電源をオンにします。
2. Cisco Secure ACS ISO イメージを持つブート可能な USB ドライブを USB ポートに差し込みます。
3. ACS を再起動して、BIOS モードに進みます。
4. BIOS モードでは、USB からのブートを選択します。
5. BIOS モードを終了して、[Save] をクリックします。
6. 再び ACS を再起動し、USB から起動します。
7. ここで、USB ドライブを使用して、Cisco SNS-3415 または Cisco SNS-3495 のイメージの再作成を続けます。

   次のメッセージが表示されます。

```
Welcome to the Cisco Secure ACS 5.8.1 Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS Installation (Keyboard/Monitor)
[2] Cisco Secure ACS Installation (Serial Console)
[3] Reset administrator password (Keyboard/Monitor
[4] Reset administrator password (Serial Console)
<Remove USB key and reboot to boot existing Hard Disk>
Please enter boot option and press <Enter>
boot:
```

8. ブート プロンプトで、**1** を入力して、**Enter** キーを押します。
9. セットアップ モードでネットワーク設定パラメータを入力すると、アプライアンスが自動的に再起動し、シェル プロンプト モードに戻ります。
10. シェル プロンプト モードを終了します。アプライアンスが起動します。
11. インストール プロセスの確認（5 ページ）に進みます。

ブート可能な USB ドライブの作成

SNS-3415 と SNS-3495 用の ACS 5.8.1 USB インストールツール（*ACS_58_USB_Installation_tool.zip*）zip は、Cisco.com で、Cisco Secure ACS 5.8.1 の Download Software セクションからダウンロードできます。この zip ファイルにはブート可能なスクリプトが含まれ、これを抽出すると Cisco Secure Access Control System 5.8.1 をインストールするためにブート可能な USB を作成できます。

はじめる前に

- *ACS_581_USB_Installation_tool.zip* ファイルが必要です。

- 次の項目が必要になります。
  - RHEL-5 または RHEL-6 Linux マシン、CentOS 5.*x* または CentOS 6.*x*。PC または MAC を使用する場合は、Linux VM がインストールされていることを確認してください。
  - 4 GB の USB ドライブ
  - iso-to-usb.sh スクリプト
- ローカル Linux マシンのドライブへのアクセス権限が必要です。

1. USB ポートに USB ドライブを差し込みます。
2. Linux マシンのディレクトリに iso-to-usb.sh スクリプトと Cisco Secure ACS 5.8.1 ISO イメージをコピーします。
3. 次のコマンドを入力します。

   iso-to-usb.sh source_iso usb_device

   たとえば、# **./iso-to-usb.sh** *ACS_v5.8.1.0.32.iso/dev/sdc* では、**iso-to-usb.sh** はスクリプトの名前で、*ACS_v5.8.1.0.32.iso* は ISO イメージの名前で、*/dev/sdc* は USB デバイスです。

   成功したことを示す、次のメッセージが表示されます。

```
*** W A R N I N G ***
THIS SCRIPT WILL DELETE ALL EXISTING CONTENT ON YOUR USB DRIVE: /dev/sdb/
ARE YOU SURE YOU WANT TO CONTINUE? [Y/N]: y
Deleting partition table on USB drive: /dev/sdb...
Creating new partition table on USB drive: /dev/sdb...
Formatting BOOT partition: /dev/sdb1 as VFAT...
Formatting DATA partition: /dev/sdb2 as EXT2...
Copying syslinux files to USB partition: /dev/sdb1...
Copying ISO file to USB partition: /dev/sdb2...
DONE!
```

4. USB ドライブを外します。

注：**iso-to-usb.sh** コマンドを実行した後、USB ドライブは非 Linux オペレーティング システムが使用できるすべての領域を認識しない形式でパーティション化されます。Windows または MAC オペレーティング システムとの一般的な使用に対して USB ドライブを再パーティション化するには、このディレクトリでコマンドの **repurpose-usb.sh** ユーティリティを実行する必要があります。このユーティリティは再パーティション化され、一般的な使用に対して USB キーを再フォーマットします。

セットアップ プログラムの実行

ここでは、ACS サーバをインストールするためのセットアップ プロセスについて説明します。

セットアップ プログラムでは、必要なパラメータの入力を求める、対話型のコマンドライン インターフェイス（CLI）が起動されます。

管理者は、コンソールまたはダム端末とセットアップ プログラムを使用して、ACS 5.8.1 サーバの初期ネットワークを設定し、初期管理者資格情報を設定します。セットアップ プロセスは一度だけ実行する設定作業です。

ACS サーバをインストールするには、次の手順を実行します。

1. アプライアンスの電源をオンにします。

   次のセットアップ プロンプトが表示されます。

   ```
   Please type 'setup' to configure the appliance
   localhost login:
   ```

2. ログイン プロンプトで **setup** と入力し、Enter を押します。

   コンソールにパラメータのセットが表示されます。表 1（6 ページ）の説明に従ってパラメータを入力します。

注: セットアップ プロセスは、最後のセットアップ値を入力する前に、Ctrl+C を押すことでいつでも中断できます。

表 1　ネットワーク設定パラメータ

プロンプト	デフォルト	条件	説明
ホスト名	*localhost*	最初の文字は ASCII 文字である必要があります。 長さは 3 ～ 15 文字である必要があります。 有効な文字は、英数字（A ～ Z、a ～ z、0 ～ 9）とハイフン（-）で、最初の文字はアルファベットである必要があります。 **注:** AD ID ストアを使用し、同じ名前のプレフィックスで複数の ACS インスタンスを設定する場合は、ホスト名として最大 15 文字を使用して AD 機能が影響を受けないようにします。	ホスト名を入力します。
IPV4 IP Address	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	IP アドレスを入力します。
IPv4 Netmask	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なネットマスクを入力します。
IPv4 Gateway	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なデフォルト ゲートウェイを入力します。
ドメイン名	なし。ネットワーク固有	IP アドレスは入力できません。 有効な文字は、ASCII 文字、数値、ハイフン（-）、およびピリオド（.）です。	ドメイン名を入力します。
IPv4 Primary Name Server Address	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なネーム サーバ アドレスを入力します。
Add/ another nameserver	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。 **注:** ACS CLI から最大 3 つのネーム サーバを設定できます。	複数のネーム サーバを設定するには、**y** と入力します。
NTP サーバ	time.nist.gov	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレス、またはドメイン ネーム サーバにする必要があります。 **注:** ACS CLI から最大 3 つの NTP サーバを設定できます。	有効なドメイン ネーム サーバまたは IPv4 アドレスを入力します。
タイムゾーン	UTC	有効なローカル タイム ゾーンである必要があります。	有効なタイム ゾーンを入力します。

表 1　ネットワーク設定パラメータ（続き）

プロンプト	デフォルト	条件	説明
SSH サービス	なし。ネットワーク固有	なし	SSH サービスを有効にするには、**y** と入力します。
ユーザ名	admin	最初の管理ユーザの名前です。デフォルトを受け入れるか、新しいユーザ名を入力します。 ユーザ名は 3 ～ 8 文字の英数字（A ～ Z、a ～ z、0 ～ 9）にする必要があります。	ユーザ名を入力します。
Admin パスワード	なし	デフォルトのパスワードはありません。パスワードを入力します。 パスワードは最低 6 文字で、小文字、大文字、数字がそれぞれ 1 つ以上含まれている必要があります。 また、次の点に注意してください。 ■ 初期設定で設定したアカウントのユーザとパスワードの情報は大切に保管してください。 ■ これらのクレデンシャルを使用すると、ACS ハードウェア、CLI、アプリケーションを管理者として完全に制御できるため、忘れないようにして保護します。 ■ 管理者のクレデンシャルを紛失した場合、ACS 5.8.1 のインストール CD を使用してパスワードをリセットできます。	パスワードを入力します。

コンソールで、次のパラメータを入力するよう求められます。

```
localhost login: setup
Enter hostname[]: acs-server-1
Enter IP address[]: a.b.c.d
Enter IP default netmask[]: 255.255.255.255
Enter IP default gateway[]: a.b.c.d
Enter default DNS domain[]: mycompany.com
Enter primary nameserver[]: a.b.c.d
Add secondary nameserver? Y/N : n
Add primary NTP server [time.nist.gov]: a.b.c.d
Add secondary NTP server? Y/N : n
Enter system timezone[UTC]:
Enable SSH service Y/N [N] : y
Enter username [admin]: admin
Enter password:
Enter password again:
Pinging the gateway...
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing acs...
Generating configuration...
Rebooting...
```

ACS サーバのインストールが完了すると、システムは自動的に再起動します。

この時点で、セットアップ プロセスで設定した CLI ユーザ名とパスワードを使用して ACS にログインできるようになります。

注: このユーザ名とパスワードを使用して ACS にログインできるのは、CLI を通じてだけです。

注: ACS 5.8.1 の初期設定では、サーバに IPv4 IP アドレスを設定する必要があります。サーバの IPv6 IP アドレスは、初期設定完了後にのみ設定できます。

注: ACS 5.8.1 は、IPv4 と IPv6 のデュアル スタック ネットワーキングをサポートしていますが、純粋な IPv6 ネットワークはサポートしていません。

インストール プロセスの確認

インストール プロセスが正しく完了したことを確認するには、次の手順を実行します。

1. システムが再起動したら、ログイン プロンプトでセットアップ時に設定したユーザ名を入力し、Enter を押します。
2. パスワード プロンプトで、セットアップ時に設定したパスワードを入力し、Enter を押します。
3. アプリケーションが適切にインストールされていることを確認するために、**show application** コマンドを入力し、**Enter** を押します。

   コンソールに次のメッセージが表示されます。

```
<name>          <Description>
acs Cisco Secure Access Control System 5.8.1
```

4. システム プロンプトでインストールされているリリースと ACS のバージョンを確認するため、**show application version acs** コマンドを入力して Enter を押します。

   コンソールに次のメッセージが表示されます。

```
Cisco ACS VERSION INFORMATION

-----------------------------

Version : 5.8.1.4
Internal Build ID : B.462
```

注: このリリースの別のバージョンでは、Version と Internal Build ID が変更されている場合があります。

5. ACS プロセスのステータスを確認するために、システム プロンプトで **show application status acs** と入力し、**Enter** を押します。

   コンソールに次のメッセージが表示されます。

```
ACS role: PRIMARY
Process 'database'                running
Process 'management'              running
Process 'runtime'                 running
Process 'adclient'                running
Process 'ntpd'                    running
Process 'view-database'           running
Process 'view-jobmanager'         running
Process 'view-alertmanager'       running
Process 'view-collector'          running
Process 'view-logprocessor'       running
```

注: 最新の ACS パッチを入手し ACS を最新に保つには、http://software.cisco.com/download/navigator.html?i=rt を参照してください。

管理者パスワードのリセット

管理者パスワードを失ったためにシステムにログインできない場合は、ACS 5.8.1 Recovery DVD を使用して管理者パスワードをリセットできます。

注: ブート可能な USB ドライブと CIMC を使用して、管理者のパスワードをリセットすることもできます。

管理者パスワードをリセットするには、次の手順を実行します。

1. アプライアンスの電源をオンにします。
2. ACS 5.8.1 Recovery DVD を挿入します。

   コンソールに次のメッセージが表示されます。

```
Welcome to Cisco Secure ACS 5.8.1 Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS 5.8.1 Installation (Keyboard/Monitor)
[2] Cisco Secure ACS 5.8.1 Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot:
```

   管理者パスワードをリセットするには、システム プロンプトで、キーボードとビデオ モニタを使用している場合は **3** と入力し、シリアル コンソール ポートを使用している場合は **4** と入力します。

   コンソールにパラメータのセットが表示されます。

3. 表 2（9 ページ）の説明に従ってパラメータを入力します。

表 2　パスワード リセット パラメータ

パラメータ	説明
Admin username	パスワードをリセットする管理者の番号を入力します。
Password	管理者の新しいパスワードを入力します。
Verify password	パスワードを再度入力します。
Save change & Reboot	保存するには **y** と入力します。

   コンソールに次のメッセージが表示されます。

```
Admin username:
[1]:admin
[2]:admin2
[3]:admin3
Enter number of admin for password recovery:1
Password
Verify password:
Save change&reeboot? [Y/N]:
```

Cisco SNS-3415/3495 アプライアンスのイメージの再作成

CIMC またはブート可能な USB ドライブを使用して、ACS 5.8.1 を使用した Cisco SNS-3415 または Cisco SNS-3495 アプライアンスのイメージを再作成できます。

Cisco SNS-3415 または Cisco SNS-3495 アプライアンスのイメージを再作成するには、次の手順を実行します。

- CIMC を使用してイメージを再作成します。CIMC を使用したリモートからの Cisco SNS-3415/3495 アプライアンスへの ACS 5.8.1 のインストール（2 ページ）を参照してください
- ブート可能な USB ドライブを使用して、イメージを再作成します。USB ドライブを使用した Cisco SNS-3415/3495 アプライアンスへの ACS 5.8.1 のインストール（4 ページ）を参照してください

法規制の遵守

法令準拠および安全性に関する情報については、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を参照してください。

Cisco SNS 3500 サーバ上の ACS 5.8.1

Cisco SNS-3515 および Cisco SNS-3595 ハードウェア アプライアンスの導入

この章では、Cisco Secure Access Control System（Cisco SNS-3515 および Cisco SNS-3595）ハードウェアの概要を紹介します。ここでは、アプライアンス ハードウェア、主なコンポーネント、コントロール、コネクタ、前面および背面パネルの LED インジケータについて説明します。

- 製品の概要（1 ページ）
- Cisco SNS 3515 および 3595 アプライアンスの LED インジケータ（6 ページ）
- 法規制の遵守（11 ページ）

製品の概要

この項では、Cisco SNS-3515 および Cisco SNS-3595 アプライアンスの電源要件、ラックマウント ハードウェア キット、および機能について説明します。

ここでは、次の項目について説明します。

- Cisco SNS-3515 および Cisco SNS-3595 アプライアンスの概要（1 ページ）
- Cisco SNS-3515 および Cisco SNS-3595 アプライアンスのハードウェア仕様（2 ページ）
- 製品シリアル番号の場所（4 ページ）
- Cisco Product Identification ツール（4 ページ）

Cisco SNS-3515 および Cisco SNS-3595 アプライアンスの概要

Cisco SNS-3515/3595 サーバは、Web サービスから分散データベースまで、広範囲のビジネス上の負荷に対応できるパフォーマンスおよび密度のために設計されています。

Cisco SNS-3515/3595 サーバの成功を反映させたエンタープライズ クラスの Cisco SNS-3515/3595 サーバは、1-RU フォーム ファクタの Cisco Unified Computing System ポートフォリオの機能を拡張します。パフォーマンス、効率の向上を実現する Intel Xeon E5-2600 プロセッサ製品ファミリを搭載することで、Cisco SNS-3515 サーバはこれらの機能を提供します。さらに、Cisco SNS-3515/3595 サーバは、最大 256 GB の RAM、8 台のドライブ、コンパクトなパッケージで卓越したレベルのサーバ密度とパフォーマンスを提供する 2 つの 1 GbE Lights-Out Management（LOM）ポートを提供します。

Cisco SNS-3515 および Cisco SNS-3595 アプライアンスのハードウェア仕様

表 1（2 ページ）では、Cisco SNS-3515 および Cisco SNS-3595 アプライアンスのハードウェア仕様について説明します。

表 1　Cisco SNS 3515 および Cisco SNS 3595 ハードウェアの概要

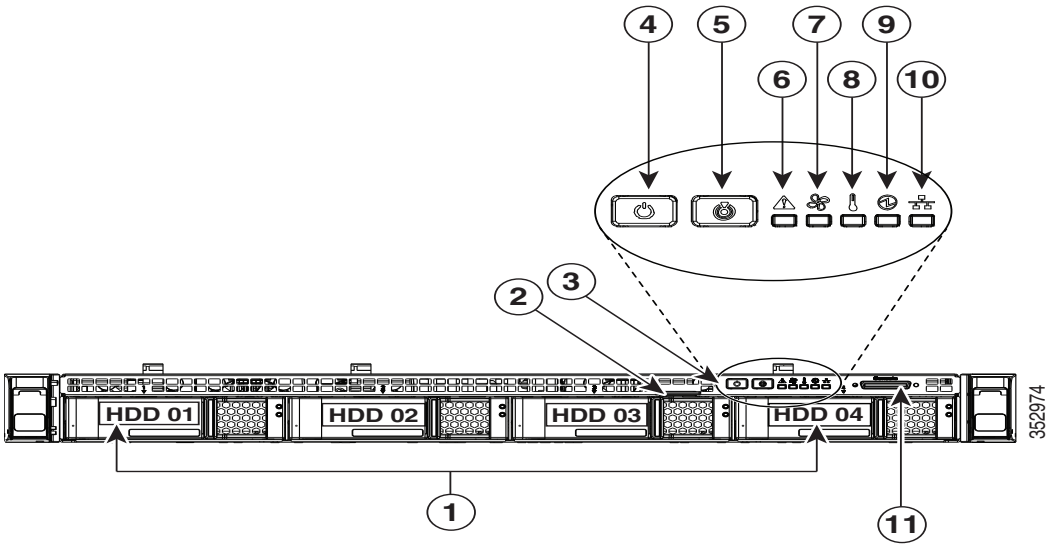
Cisco Secure ACS アプライアンス	ハードウェア仕様	図
Cisco SNS-3515-K9	■ Cisco UCS C220 M4 ■ シングル ソケット インテル Xeon E5-2620 v3 シリーズ CPU（2.40GHz、合計コア数 6、合計スレッド数 6*2） ■ 16 GB RAM ■ 600 GB ディスク x 1 ■ 組み込みソフトウェア RAID 0 ■ 6 GbE ネットワーク インターフェイス ■ 物理的仕様、環境仕様、および電源仕様については、サーバの仕様（4 ページ）を参照してください。	■ 図 1（3 ページ）に Cisco SNS-3515 アプライアンスを示します。（2 ページ） ■ 図 2Cisco SNS-3515/3595 アプライアンスの背面図（3 ページ）
Cisco SNS-3595-K9	■ Cisco UCS C220 M4 ■ デュアル ソケット インテル Xeon E5-2640 v3 シリーズ CPU（2.60GHz、合計コア数 8、合計スレッド数 8*2） ■ 64 GB RAM ■ 600 GB ディスク x 4 ■ RAID 10 ■ 6 GbE ネットワーク インターフェイス ■ 物理的仕様、環境仕様、および電源仕様については、サーバの仕様（4 ページ）を参照してください。	■ 図 1Cisco SNS-3595/3515 アプライアンスの正面図（3 ページ） ■ 図 2Cisco SNS-3515/3595 アプライアンスの背面図（3 ページ）

注：ACS 5.8.1 は、Cisco SNS-3515-K9 のオプションの冗長電源装置をサポートします。

シャーシの正面図

図 1（3 ページ）に Cisco SNS-3515 アプライアンスを示します。

図 1　Cisco SNS-3595/3515 アプライアンスの正面図

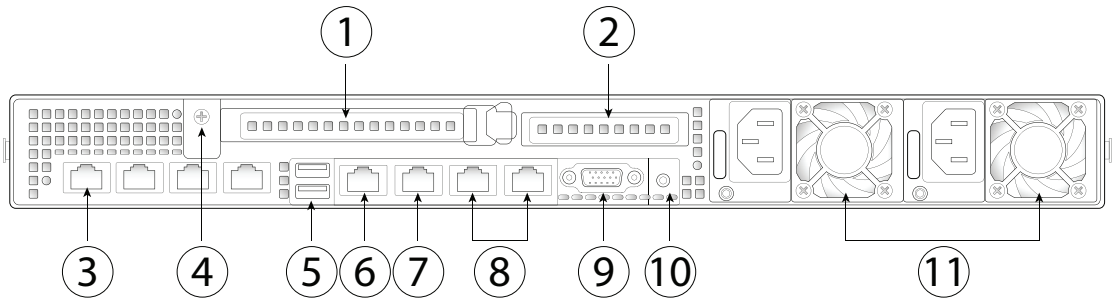


1	ドライブ（最大 4 台の 2.5 インチ ドライブ）	7	ファン ステータス LED
2	引き抜きアセット タグ	8	温度ステータス LED
3	操作パネル ボタンおよび LED	9	電源装置ステータス LED
4	電源ボタン/電源ステータス LED	10	ネットワーク リンク アクティビティ LED
5	ユニット識別ボタン/LED	11	KVM コネクタ（USB 2.0 2 個、VGA 1 個、シリアル コネクタ 1 個を装備した KVM ケーブルで使用）
6	システム ステータス LED		

シャーシの背面図

図 2（3 ページ） に、Cisco SNS-3515 アプライアンスと Cisco SNS-3595 アプライアンスの背面パネルの外部機能を示します。

図 2　Cisco SNS-3515/3595 アプライアンスの背面図



1	PCIe ライザ 1/スロット 1	7	シリアル ポート（RJ-45 コネクタ）
2	PCIe ライザ 2/スロット 2	8	デュアル 1 GbE イーサネット ポート（LAN1 と LAN2）
3	モジュラ LAN-on-motherboard（mLOM）カード スロット	9	VGA ビデオ ポート（DB-15）
4	アース ラグの穴（DC 電源ユニットの場合）	10	背面ユニット識別ボタン/LED
5	USB 3.0 ポート（2 個）	11	電源ユニット（最大 2 台、1+1 冗長）
6	1 GbE イーサネット専用管理ポート		

製品シリアル番号の場所

シリアル番号ラベルは、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの前面パネルのサーバの上部にあります。（2 ページ） に、このラベルの場所を示します。

Cisco Product Identification ツール

Cisco 製品 ID（CPI）ツールは、シスコ製品のシリアル番号を取得する際に役立ちます。

オンラインまたは電話でサービスのリクエスト要求をする前に、CPI ツールを使用して製品のシリアル番号を検索します。このツールは、シスコのサポート Web サイトからアクセスできます。

ツールにアクセスする方法は、次のとおりです。

1. [Get Tools & Resources] リンクをクリックします。
2. [All Tools (A-Z)] タブをクリックします。
3. アルファベット順のドロップダウン リストから [Cisco Product Identification Tool] を選択します。

   このツールには、3 つの検索オプションがあります。

- 製品 ID またはモデル名による検索。
- シスコ モデルの参照。
- **show** コマンドで出力をコピー アンド ペーストして製品を特定。

  検索結果では、製品画像とともにシリアル番号ラベルの場所が強調表示されます。製品のシリアル番号ラベルのある場所を探し、サービスに問い合わせる前にその情報を記録します。

  CPI ツールは、次の URL からアクセスできます。

  http://tools.cisco.com/Support/CPI/index.do

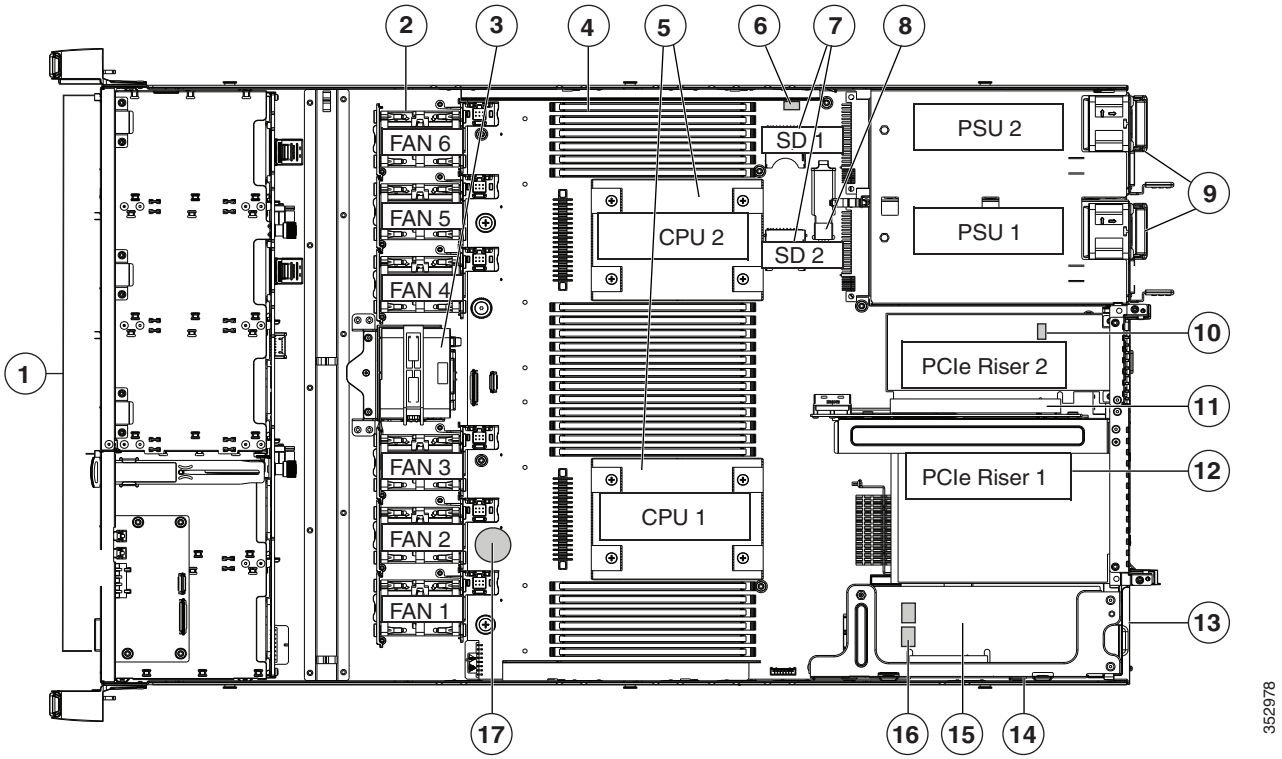
  CPI ツールにアクセスするには、Cisco.com ユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

  http://tools.cisco.com/RPF/register/register.do

交換可能なコンポーネントの位置

この項では、現場で交換可能なコンポーネントの位置を示します。図 1-4 は、上から見下ろした図です。上部カバーとエアーバッフルは取り外してあります。

図 3　交換可能なコンポーネントの位置



1	ドライブ（SAS/SATA ドライブはホットスワップ可能）	10	マザーボード上のトラステッド プラットフォーム モジュール（TPM）ソケット（図に非表示）
2	冷却ファン モジュール（6 個）	11	PCIe ライザー 2（ハーフハイト PCIe スロット 2）
3	Super cap 電源モジュール（RAID バックアップ）の取り付けブラケット	12	PCIe ライザー 1（フルハイト PCIe スロット 1）
4	マザーボード上の DIMM スロット（24 個）	13	シャーシ フロア上のモジュラ LOM（mLOM）コネクタ
5	CPU とヒートシンク（最大 2 セット）	18	シスコ モジュラ RAID コントローラ PCIe ライザー（水平ソケット搭載の専用ライザー）
6	RAID 5 キー用組み込み SATA RAID ヘッダー	15	シスコ モジュラ RAID コントローラ カード
7	マザーボード上の SD カード ベイ（2 個）	16	マザーボード上の組み込み SATA RAID mini-SAS コネクタ（図に非表示）
8	マザーボード上の内部 USB 3.0 ポート	17	マザーボード上の RTC バッテリ
9	電源ユニット（最大 2 台、1+1 冗長な場合にホットスワップ可能）		

Cisco SNS 3515 および 3595 アプライアンスの LED インジケータ

この項では、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの前面および背面パネルのコントロール、ポート、および LED インジケータについて説明します。

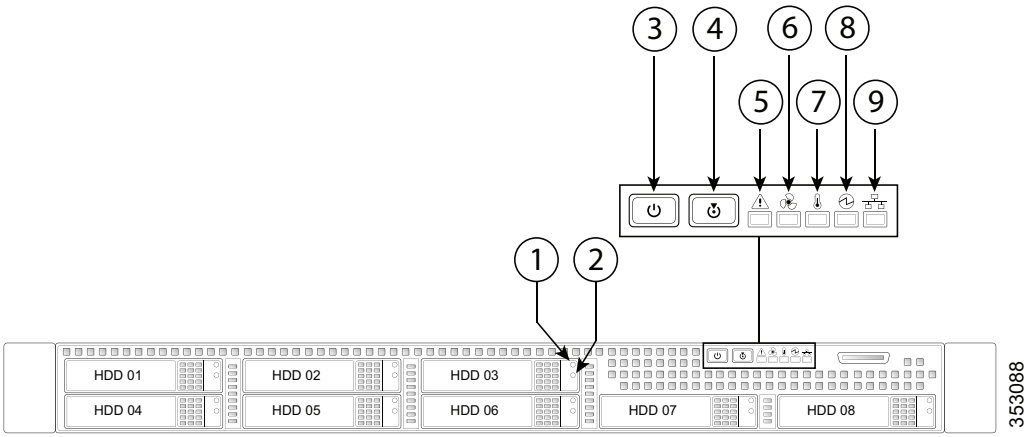
ここでは、次の項目について説明します。

- Cisco SNS-3515 または 3595 アプライアンスの前面パネル図（6 ページ）
- Cisco SNS-3515/3595 アプライアンスの背面パネル ビュー（8 ページ）
- 内部診断 LED（10 ページ）

Cisco SNS-3515 または 3595 アプライアンスの前面パネル図

図 4（6 ページ）に Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの前面パネル ビューのコンポーネントを示します。

図 4　前面パネル LED



1	ハード ドライブ障害 LED	6	ファン ステータス LED
2	ハード ドライブ動作 LED	7	温度ステータス LED
3	電源ボタン/電源ステータス LED	8	電源装置ステータス LED
4	ID ボタン/LED	9	ネットワーク リンク アクティビティ LED
5	システム ステータス LED	10	

表 2(7 ページ) では、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの前面パネルに配置された LED について説明します。

表 2　前面パネルの LED

LED 名	状態
ハード ドライブ障害 注:コントローラが Cisco UCS RAID SAS 9300-8i または 9300-8e HBA である場合は、異なる LED 動作について「Cisco UCS SAS 9300-8i and 9300-8e HBA Considerations」を参照してください。	■ 消灯:ハード ドライブは正常に動作中です。 ■ オレンジ:ドライブ障害が検出されました。 ■ オレンジの点滅:デバイスの再構成中です。 ■ 1 秒間隔のオレンジの点滅:ドライブ位置特定機能はアクティブです。
ハード ドライブ アクティビティ	■ 消灯:ハード ドライブ トレイにハード ドライブが存在しません(アクセスなし、障害なし)。 ■ 緑:ハード ドライブの準備が完了しています。 ■ 緑の点滅:ハード ドライブはデータの読み取り中または書き込み中です。
電源ボタン/LED	■ 消灯:サーバに AC 電力が供給されていません。 ■ オレンジ:サーバはスタンバイ電源モードです。Cisco IMC と一部のマザーボード機構にだけ電源が投入されています。 ■ 緑:サーバは主電源モードです。すべてのサーバ コンポーネントに電力が供給されています。
ユニット識別	■ 消灯:ユニット識別機能は使用されていません。 ■ 青:ユニット識別機能はアクティブです。
システム ステータス	■ 緑:サーバは正常動作状態で稼働しています。 ■ 緑の点滅:サーバはシステムの初期化とメモリ チェックを行っています。 ■ オレンジの点灯:サーバは縮退運転状態にあります。次に例を示します。 – 電源装置の冗長性が失われている。 – CPU が一致しない。 – 少なくとも 1 つの CPU に障害が発生している。 – 少なくとも 1 つの DIMM に障害が発生している。 – RAID 構成内の少なくとも 1 台のドライブに障害が発生している。 ■ オレンジの点滅:サーバは重大な障害発生状態にあります。次に例を示します。 – ブートに失敗した。 – 修復不能な CPU またはバス エラーが検出された。 – サーバが過熱状態にある。

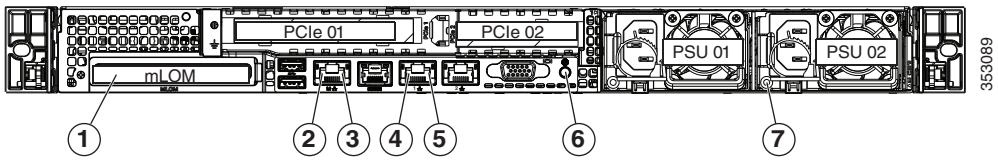
表 2　前面パネルの LED（続き）

LED 名	状態
ファン ステータス	■ 緑：すべてのファン モジュールが正常に動作中です。 ■ オレンジの点灯：1 つ以上のファン モジュールで重大なしきい値を超えました。 ■ オレンジの点滅：1 つ以上のファン モジュールで回復不能なしきい値を超えました。
温度ステータス	■ 緑：サーバは正常温度で稼働中です。 ■ オレンジの点灯：1 つ以上の温度センサーで重大なしきい値を超えました。 ■ オレンジの点滅：1 つ以上の温度センサーで回復不能なしきい値を超えました。
電源ステータス	■ 緑：すべての電源装置が正常に動作中です。 ■ オレンジの点灯：1 台以上の電源装置が縮退運転状態にあります。 ■ オレンジの点滅：1 台以上の電源装置が重大な障害発生状態にあります。
ネットワーク リンク アクティビティ	■ 消灯：イーサネット リンクがアイドル状態です。 ■ 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 ■ 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。

Cisco SNS-3515/3595 アプライアンスの背面パネル ビュー

図 2（3 ページ） に Cisco SNS-3515 アプライアンスおよび Cisco 3595 アプライアンスの背面パネル ビューのコンポーネントを示します。

図 5　前面パネル LED



1	オプションの mLOM カード LED（表 3（9 ページ） を参照してください）。	5	1 GbE イーサネット リンク ステータス LED
2	1 GbE イーサネット専用管理リンク ステータス LED	6	背面ユニット識別ボタン/LED
3	1 GbE イーサネット専用管理リンク速度 LED	7	電源装置ステータス LED
4	1 GbE イーサネット リンク速度 LED		

表 3（9 ページ）では、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの前面パネルに配置された LED について説明します。

表 3　背面パネルの LED

LED 名	状態
オプションの mLOM 1-GbE SFP+ （ステータス LED が 1 つだけあります）	■ 消灯：リンクが確立されていません。 ■ 緑の点灯：リンクはアクティブです。 ■ 緑の点滅：アクティブなリンクにトラフィックが存在します。
オプションの mLOM 1-GbE BASE-T リンク速度	■ 消灯：リンク速度は 10 Mbps です。 ■ オレンジ：リンク速度は 100 Mbps/1 Gbps です。 ■ 緑：リンク速度は 10 Gbps です。
オプションの mLOM 1-GbE BASE-T リンク ステータス	■ 消灯：リンクが確立されていません。 ■ 緑：リンクはアクティブです。 ■ 緑の点滅：アクティブなリンクにトラフィックが存在します。
1 GbE イーサネット専用管理リンク速度	■ 消灯：リンク速度は 10 Mbps です。 ■ オレンジ：リンク速度は 100 Mbps です。 ■ 緑：リンク速度は 1 Gbps です。
1-GbE イーサネット専用管理リンク ステータス	■ 消灯：リンクが確立されていません。 ■ 緑：リンクはアクティブです。 ■ 緑の点滅：アクティブなリンクにトラフィックが存在します。
1-GbE イーサネット リンク速度	■ 消灯：リンク速度は 10 Mbps です。 ■ オレンジ：リンク速度は 100 Mbps です。 ■ 緑：リンク速度は 1 Gbps です。
1-GbE イーサネット リンク ステータス	■ 消灯：リンクが確立されていません。 ■ 緑：リンクはアクティブです。 ■ 緑の点滅：アクティブなリンクにトラフィックが存在します。
背面ユニット識別	■ 消灯：ユニット識別 LED は使用されていません。 ■ 青：ユニット識別 LED はアクティブです。
電源ステータス	AC 電源： ■ 消灯：AC 入力なし（12 V 主電源はオフ、12 V スタンバイは電源オフ）です。 ■ 緑の点滅：12 V 主電源はオフ、12 V スタンバイ電源はオンです。 ■ 緑の点灯：12 V 主電源はオン、12 V スタンバイ電源はオンです。 ■ オレンジの点滅：警告が検出されましたが、12 V 主電源はオンです。 ■ オレンジの点灯：重大なエラーが検出され、12 V 主電源はオフです。

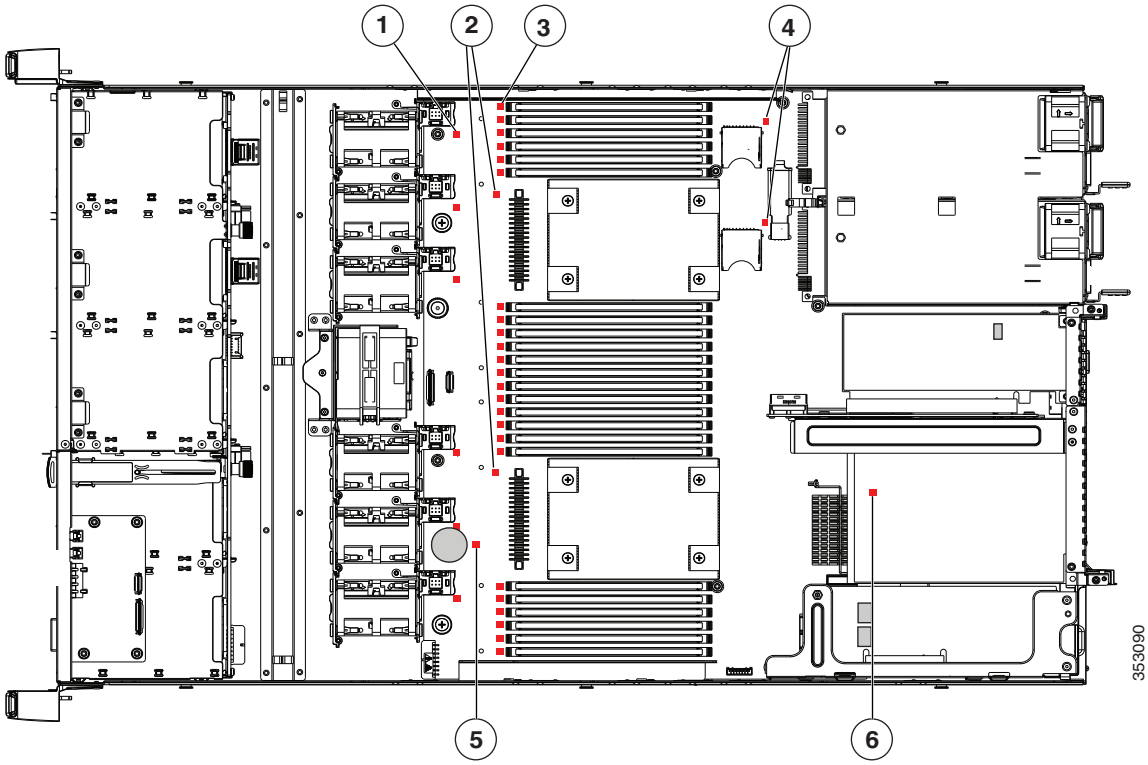
内部診断 LED

サーバには、CPU、DIMM、ファン モジュール、SD カード、RTC バッテリ、および mLOM カードの内部障害 LED があります。これらの LED は、サーバがスタンバイ電源モードの場合にのみ使用できます。障害が発生しているコンポーネントの LED がオレンジに点灯します。

注: これらの LED が動作するには、サーバに電源が接続されている必要があります。

図 6（10 ページ） に Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの内部 LED の位置を示します。

図 6　Cisco SNS-3515 または 3595 の内部診断 LED の位置



次の表で、図 6（10 ページ） の各コンポーネントについて説明します。

1	ファン モジュール障害 LED（マザーボード上の各ファン コネクタの隣に 1 個）	4	SD カード障害 LED（各ベイの横に 1 個）
2	CPU 障害 LED（各 CPU の前に 1 個）	5	RTC バッテリ障害 LED
3	DIMM 障害 LED（マザーボード上の各 DIMM ソケットの前に 1 個）	6	mLOM カード障害 LED（mLOM ソケットの横のマザーボード上）

表 4（10 ページ） では、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスに搭載された内部診断 LED について説明します。

表 4　内部診断 LED

LED 名	状態
内部診断 LED（すべて）	■ 消灯：コンポーネントは正常に機能しています。 ■ オレンジ：コンポーネントに障害が発生しています。

法規制の遵守

法令準拠および安全性に関する情報については、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を参照してください。

詳細については、マニュアルの入手方法およびテクニカル サポート（11 ページ）を参照してください。

法規制の遵守

Cisco SNS 3515 および Cisco SNS 3595 ハードウェア アプライアンスの設置の準備

ここでは、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスを安全に設置するために場所を準備する方法について説明します。

ここでは、次の項目について説明します。

- 安全に関する注意事項（1 ページ）
- サーバの開梱と点検（2 ページ）
- サーバの設置準備（3 ページ）
- サーバの仕様（4 ページ）

安全に関する注意事項

注：Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの設置、操作、または保守を行う前に、安全上の重要事項について、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を確認します。

警告：**安全上の重要事項**

「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。
ステートメント 1071

警告：**システムの過熱を防ぐため、最大推奨周囲温度の 40°C（104°F）を超えるエリアで操作しないでください。**
ステートメント 1047

警告：**いつでも装置の電源を切断できるように、プラグおよびソケットにすぐに手が届く状態にしておいてください。**
ステートメント 1019

警告：**この製品は、設置する建物に短絡（過電流）保護機構が備わっていることを前提に設計されています。この保護装置の定格が 250 V、15 A 以下であることを確認します。**
ステートメント 1005

警告：**装置は地域および国の電気規則に従って設置する必要があります。**
ステートメント 1074

サーバを設置する際には、次のガイドラインに従ってください。

- サーバを設置する前に、設置場所の構成を計画し、設置環境を整えます。設置場所を計画する際に推奨される作業については、『*Cisco UCS Site Preparation Guide*』を参照してください。
- サーバの周囲に、保守作業および適切な通気のための十分なスペースがあることを確認します。サーバ内では前面から背面へ空気が流れます。

- 空調が、サーバの仕様（4 ページ）に記載された温度要件に適合していることを確認します。
- キャビネットまたはラックが、ラックに関する要件（4 ページ）に記載された要件に適合していることを確認します。
- 設置場所の電源が、サーバの仕様（4 ページ）に記載された電源要件に適合していることを確認します。使用可能な場合は、電源障害に備えて無停電電源装置（UPS）を使用してください。

注意：鉄共振技術を使用する UPS タイプは使用しないでください。このタイプの UPS は、Cisco UCS などのシステムに使用すると、データ トラフィック パターンの変化によって入力電流が大きく変動し、動作が不安定になるおそれがあります。

サーバの開梱と点検

注意：サーバの内部コンポーネントを取り扱うときは ESD ストラップを使用し、モジュールは端の部分を持ってください。

注：サーバの輸送が必要となる場合に備えて、輸送用の箱は保管しておいてください。

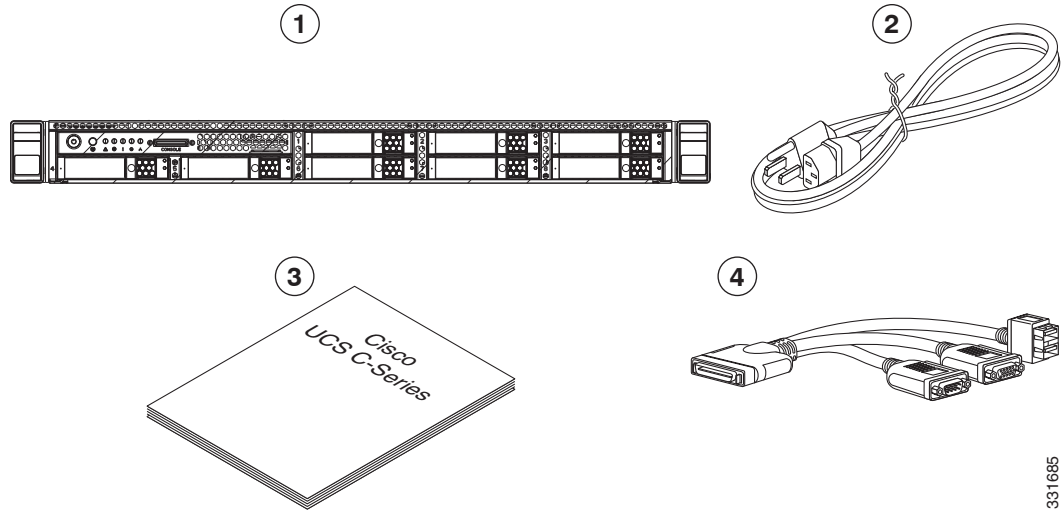
注：シャーシは厳密に検査したうえで出荷されています。輸送中の破損や内容品の不足がある場合には、ただちにカスタマー サービス担当者に連絡してください。

梱包内容を確認する手順は、次のとおりです。

1. 段ボール箱からサーバを取り出します。梱包材はすべて保管しておいてください。
2. カスタマー サービス担当者から提供された機器リストおよび図 1（2 ページ）と、梱包品の内容を照合します。すべての品目が揃っていることを確認してください。
3. 破損の有無を調べ、内容品の間違いや破損がある場合には、カスタマー サービス担当者に連絡してください。次の情報を用意しておきます。

- 発送元の請求書番号（梱包明細を参照）
- 破損している装置のモデルとシリアル番号
- 破損状態の説明
- 破損による設置への影響

図 1　梱包内容



1	サーバ	3	資料
2	電源コード（オプション、最大 2 本）	4	KVM ケーブル

サーバの設置準備

ここでは、サーバの設置準備について説明します。この項の内容は次のとおりです。

- 設置に関するガイドライン（3 ページ）
- ラックに関する要件（4 ページ）
- 機器の要件（4 ページ）
- スライド レールの調整範囲（4 ページ）

設置に関するガイドライン

警告：システムの過熱を防ぐため、最大推奨周囲温度の 40°C（104°F）を超えるエリアで操作しないでください。
ステートメント 1047

警告：いつでも装置の電源を切断できるように、プラグおよびソケットにすぐに手が届く状態にしておいてください。
ステートメント 1019

警告：この製品は、設置する建物に短絡（過電流）保護機構が備わっていることを前提に設計されています。この保護装置の定格が 250 V、15 A 以下であることを確認します。
ステートメント 1005

警告：装置は地域および国の電気規則に従って設置する必要があります。
ステートメント 1074

注意：鉄共振技術を使用する UPS タイプは使用しないでください。このタイプの UPS は、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスなどのシステムに使用すると、データ トラフィック パターンの変化によって入力電流が大きく変動し、動作が不安定になることがあります。

注意：サーバを取り付ける際は、適切なエアーフローを確保するために、レール キットを使用する必要があります。レール キットを使用せずに、ユニットを別のユニットの上に物理的に置く、つまり「積み重ねる」と、サーバの上部にある通気口がふさがれ、過熱したり、ファンの回転が速くなったり、電力消費が高くなったりする原因となる可能性があります。サーバをラックに取り付けるときは、これらのレールによりサーバ間で必要な最小の間隔が提供されるので、レール キットにサーバをマウントすることを推奨します。レール キットを使用してユニットをマウントする場合は、サーバ間の間隔を余分にとる必要はありません。

サーバを設置する際には、次のガイドラインに従ってください。

- サーバを設置する前に、設置場所の構成を計画し、設置環境を整えます。設置場所を計画する際に推奨される作業については、『*Cisco UCS Site Preparation Guide*』を参照してください。
- サーバの周囲に、保守作業および適切な通気のための十分なスペースがあることを確認します。サーバ内では前面から背面へ空気が流れます。
- 空調が、サーバの仕様（4 ページ）に記載された温度要件に適合していることを確認します。
- キャビネットまたはラックが、ラックに関する要件（4 ページ）の項に記載された要件に適合していることを確認します。
- 設置場所の電源が、サーバの仕様（4 ページ）に記載された電源要件に適合していることを確認します。使用可能な場合は、電源障害に備えて無停電電源装置（UPS）を使用してください。

ラックに関する要件

ここでは、標準的なオープン ラックの要件について説明します。

次のタイプのラックを使用する必要があります。

- 標準的な 19 インチ（48.3 cm）幅 4 支柱 EIA ラック（ANSI/EIA-310-D-1992 のセクション 1 に準拠した英国ユニバーサル ピッチに適合するマウント支柱付き）。
- 付属のスライド レールを使用する場合、ラック支柱の穴は、0.38 インチ（9.6 mm）の正方形、0.28 インチ（7.1 mm）の丸形、#12-24 UNC、または #10-32 UNC になります。
- サーバあたりの縦方向の最小ラック スペースは、1 RU、つまり 1.75 インチ（44.45 mm）である必要があります。

機器の要件

このサーバ用にシスコから提供されるスライド レールの場合、取り付けに必要な工具はありません。内側のレール（取り付けブラケット）が、サーバの側面にあらかじめ取り付けられています。

スライド レールの調整範囲

このサーバのスライド レールの調整範囲は 24 ～ 36 インチ（610 ～ 914 mm）です。

サーバの仕様

ここでは、サーバの技術仕様について説明します。内容は次のとおりです。

- 物理的仕様（4 ページ）
- 環境仕様（4 ページ）
- 電源仕様（5 ページ）

物理的仕様

表 1（4 ページ）に、サーバの物理的仕様を示します。

表 1　物理的仕様

説明	仕様
高さ	4.3 cm（1.7 インチ）
幅	42.9 cm（16.9 インチ）
奥行き	75.8 cm（29.8 インチ）
重量（フル装備のシャーシ）	SNS 3515：17.2 kg（37.9 ポンド） SNS 3595：18.1 kg（39.9 ポンド）

環境仕様

表 2（5 ページ）に、サーバの環境仕様を示します。

表 2　環境仕様

説明	仕様
動作時温度	41 ～ 104°F（5 ～ 40°C） 海抜 305 m ごとに最高温度が 1°C 低下。
非動作時温度（サーバが倉庫にあるか運送中の場合）	-40 ～ 149°F（-40 ～ 65°C）
湿度（RH）、結露なし	10 ～ 90 %
動作時高度	0 ～ 3,048 m（0 ～ 10,000 フィート）
非動作時高度	0 ～ 12,192 m（0 ～ 40,000 フィート）
音響出力レベル ISO7779 に基づく A 特性音響出力レベル LwAd（Bels）を測定 23 °C（73 °F）で動作	5.4
騒音レベル ISO7779 に基づく A 特性音圧レベル LpAm（dBA）を測定 23 °C（73 °F）で動作	37

電源仕様

電源オプションの電源仕様を次に示します。

- 770-WAC 電源（5 ページ）

次の URL にある Cisco UCS Power Calculator を使用すると、ご使用のサーバ設定の電源に関する詳細情報を取得できます。

http://www.cisco.com/assets/cdc_content_elements/flash/dataCenter/cisco_ucs_power_calculator/

注：サーバに異なる種類の電源を混在させないでください。両方の電源装置が同じである必要があります。

注：ACS 5.8.1 は、Cisco SNS-3515-K9 のオプションの冗長電源装置をサポートします。

770-WAC 電源

表 3（5 ページ） に、サーバの環境仕様を示します。

表 3　電源ユニットの仕様

説明	仕様
AC 入力電圧範囲	90 ～ 264 VAC（自己調整、公称 100 ～ 264 VAC）
AC 入力周波数	範囲：47 ～ 63 Hz（単相、公称 50 ～ 60Hz）
AC 回線入力電流（定常ステート）	9.5 A（100 VAC で最大） 4.5 A（208 VAC で最大）
各電源装置の最大出力電力	770W
電源装置の出力電圧	主電源：12 VDC スタンバイ電源：12 VDC

サーバの仕様

Cisco SNS 3515 および Cisco SNS 3595 ハードウェア アプライアンスの設置

この章では、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの設置方法とネットワークへの接続方法について説明します。

内容は、次のとおりです。

- Cisco SNS-3515/3595 アプライアンス ラックの設置（1 ページ）
- Cisco Integrated Management Controller（CIMC）（10 ページ）
- ケーブルの接続（5 ページ）
- Cisco SNS-3515 または 3595 アプライアンスの接続と電源投入（8 ページ）

設置を始める前に、『*Regulatory Compliance and Safety Information for the Cisco 3515 or 3595 Secure Access Control System*』を参照してください。

警告：この装置の設置、交換、または保守は、訓練を受けた、適格である人が行ってください。ステートメント 1030

警告：この装置は、立ち入りが制限された場所への設置を前提としています。立ち入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段を使用しないと入室できない場所を意味します。
ステートメント 1017

Cisco SNS-3515/3595 アプライアンス ラックの設置

ここでは、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスをラックに設置する方法について説明します。次のセクションで構成されています。

- サイド レールの取り付け（1 ページ）
- ケーブル マネジメント アーム（省略可能）の取り付け（4 ページ）
- ケーブル マネジメント アーム（省略可能）の取り付けを逆にする（5 ページ）

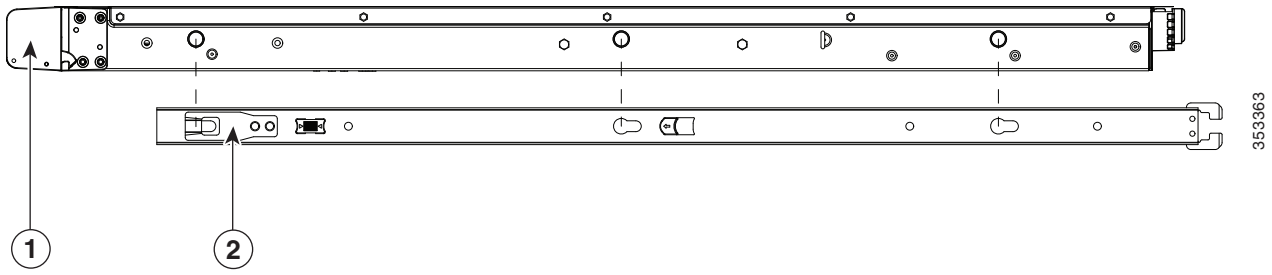
サイド レールの取り付け

警告：ラックへのユニットの設置や、ラック内のユニットの保守作業を行う場合は、負傷事故を防ぐため、システムが安定した状態で置かれていることを十分に確認してください。安全を確保するために、次の注意事項を守ってください。
ラックに設置する装置が 1 台だけの場合は、ラックの一番下に取り付けます。
ラックにすでに他の装置が搭載されている場合は、最も重いコンポーネントをラックの一番下にして、重い順に下から上へと搭載するようにしてください。
ラックにスタビライザが付いている場合は、スタビライザを取り付けてから、ラックに装置を設置したり、ラック内の装置を保守したりしてください。
ステートメント 1006

スライド レールとサーバをラックに取り付けるには、次の手順に従います。

1. サーバの側面に内側レールを装着します。
   a. レール内の 3 つのキー付きスロットがサーバ側面の 3 個のペグの位置に合うように、内側レールをサーバの一方の側の位置に合わせます（図 1（2 ページ）を参照）。
   b. キー付きスロットをペグに設定し、レールを前面に向けてスライドさせて、ペグの所定の位置にロックします。前面スロットには、前面ペグにロックするための金属製クリップがあります。
   c. 2 つ目の内側レールをサーバの反対側に取り付けます。

図 1　サーバの側面への内側レールの装着

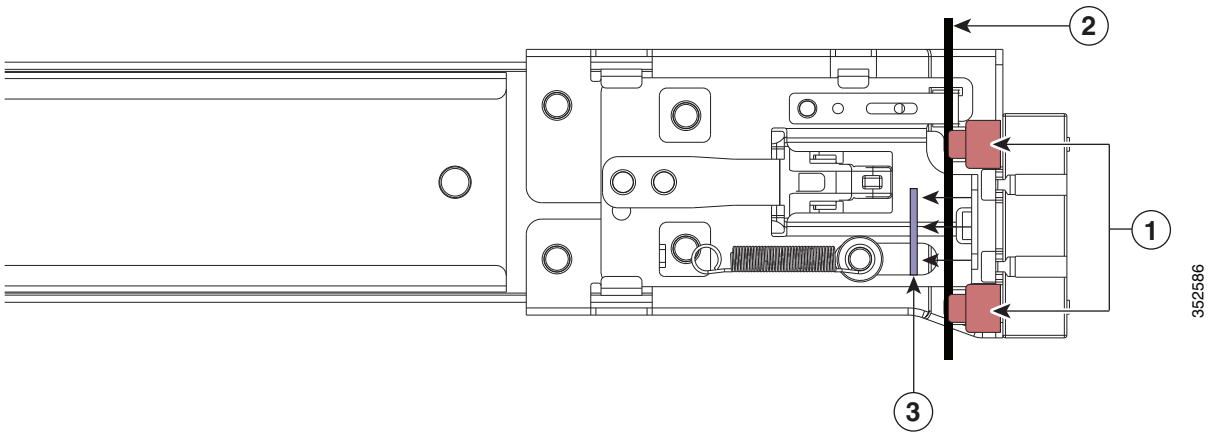


1	サーバの前面	2	内側レールのロッキング クリップ

2. 両方のスライド レール部品で前面の固定プレートを開きます。スライド レール部品の前端に、バネ仕掛けの固定プレートがあります。取り付けペグをラック支柱の穴に挿入する前に、この固定プレートが開いている必要があります（図 2（2 ページ）を参照）。

   部品の外側で、背面を向いている緑色の矢印ボタンを押して、固定プレートを開きます。

図 2　前面の固定部分、前端の内側



1	前面側の取り付けペグ	3	開いた位置に引き戻された固定プレート
2	ラック支柱		

3. 外側のスライド レールをラックに取り付けます。

   a. 片側のスライド レール部品の前端を、使用する前面ラック支柱の穴の位置に合わせます。

   スライド レールの前端をラック支柱の外側に迂回させ、取り付けペグを外側前面からラック支柱の穴に入れます（図 2（2 ページ）を参照）。

   注：ラック支柱は、取り付けペグと開いた固定プレートの間にある必要があります。

   b. 取り付けペグを、外側前面からラック支柱の穴に差し込みます。

   c. 「PUSH」のマークが付いた固定プレートのリリース ボタンを押します。ばね仕掛けの固定プレートが閉じて、ペグが所定の位置にロックされます。

   d. スライド レールの長さを調整したら、背面取り付けペグを対応する背面ラック支柱の穴に差し込みます。スライド レールは前面から背面に向かって水平である必要があります。

   背面取り付けペグを、ラック支柱の内側から背面ラック支柱の穴に入れます。

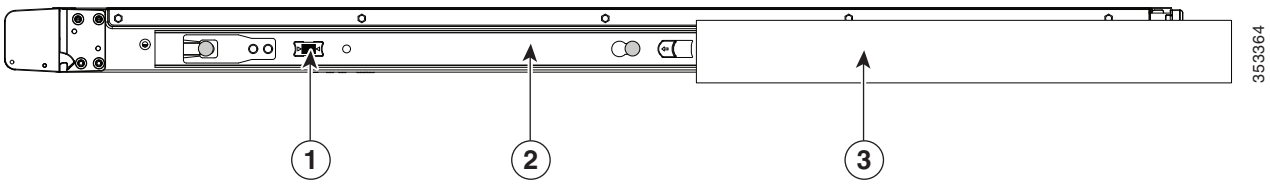
   e. 2 つ目のスライド レール部品を、ラックの反対側に取り付けます。2 つのスライド レール部品が相互に同じ高さであり、水平になっていることを確認します。

   f. f. 所定の位置に収まって留まるまで、各部品の内側のスライド レールをラック前方へ引き出します。

4. サーバを次のようにスライド レールに装着します。

注意：このサーバは、コンポーネントがフルに搭載されている場合、最大で 59 kg（67 ポンド）の重量になる場合があります。サーバを持ち上げるときは、2 人以上で行うか、リフトを使用することを推奨します。この手順を 1 人で実行しようとすると、怪我や機器の損傷を招くおそれがあります。

図 3　内側レールのリリース クリップ



1	内側レールのリリース クリップ	3	ラック支柱に装着されている外側レール
2	サーバに装着され、外側レールに挿入されている内側レール		

5. （任意）スライド レールに付属の 2 本のネジを使用して、サーバをさらに確実にラックに固定します。サーバを取り付けたラックを移動する場合は、この手順を実行します。

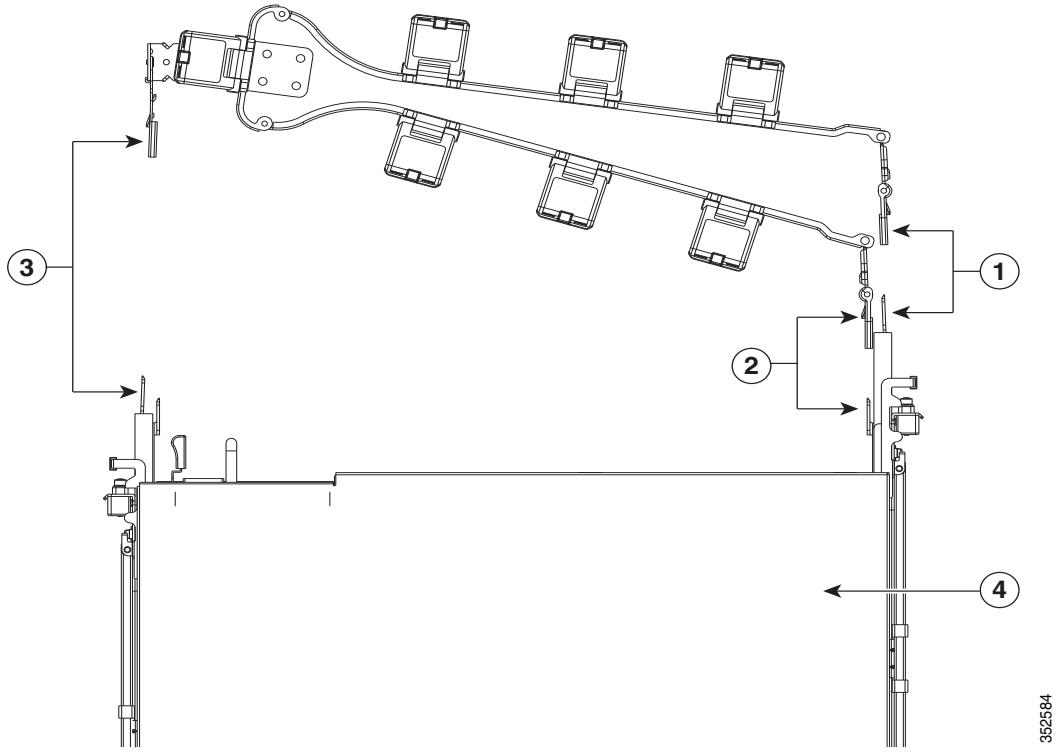
   サーバをスライド レールに完全に押し込んだ状態で、サーバ前面のヒンジ付きスラム ラッチのレバーを開き、レバーの下にある穴からネジを挿入します。ネジがラック支柱のレールの静止部分に挿入され、サーバが引き抜かれるのを防ぎます。反対のスラム ラッチについても行ってください。

ケーブル マネジメント アーム（省略可能）の取り付け

注:CMA は左右逆に取り付けることもできます。CMA を逆に取り付けるには、取り付け前に「ケーブル マネジメント アームを逆に取り付ける（省略可）」を参照してください。

1. サーバをラックに完全に押し込んだ状態で、サーバから最も離れた CMA アームの CMA タブを、ラック支柱に装着された固定スライド レールの終端にスライドさせます（図 4（4 ページ） を参照）。カチッと音がしてロックされるまで、タブをレールの終端にスライドさせます。
2. サーバに最も近い CMA タブを、サーバに装着された内側レールの終端にスライドさせます（図 4（4 ページ） を参照）。カチッと音がしてロックされるまで、タブをレールの終端にスライドさせます。
3. ラックの幅に一致するまで、CMA アセンブリの反対側の終端にある幅調整スライダを引き出します（図 4（4 ページ） を参照）。
4. 幅調整スライダの終端にある CMA タブを、ラック支柱に装着された固定スライド レールの終端にスライドさせます（図 4（4 ページ） を参照）。カチッと音がしてロックされるまで、タブをレールの終端にスライドさせます。
5. 各プラスチック製ケーブル ガイドの上部でヒンジ付きフラップを開き、必要に応じてケーブル ガイドを通してケーブルを配線します。

図 4　スライド レールの背面へのケーブル マネジメント アームの装着

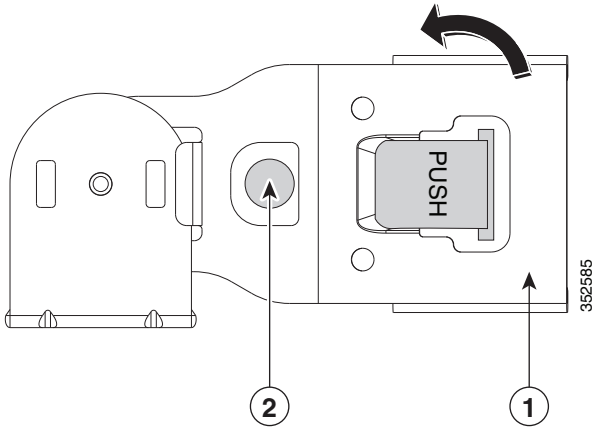


1	サーバから最も離れたアームの CMA タブと外側の固定スライド レールの終端	3	幅調整スライダの CMA タブと外側の固定スライド レールの終端
2	サーバに最も近いアームの CMA タブとサーバに装着された内側のスライド レールの終端	4	サーバ背面

ケーブル マネジメント アーム（省略可能）の取り付けを逆にする

1. CMA アセンブリ全体を 180 度回転させます。プラスチック製ケーブル ガイドは、上を向いたままにしておく必要があります。
2. サーバの背面を向くように、各 CMA アームの終端でタブを反転させます。
3. 幅調整スライダの終端にあるタブを回転させます。タブの外側の金属ボタンを長押しし、サーバの背面を向くようにタブを 180 度回転させます。

図 5　CMA の反転



1	幅調整スライダの終端の CMA タブ	3	回転用金属ボタン

ケーブルの接続

ここでは、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスをネットワークおよびアプライアンス コンソールに接続する方法について説明します。この項では、次の内容について説明します。

- ネットワーク インターフェイスの接続（5 ページ）
- コンソールの接続（7 ページ）
- キーボードとビデオ モニタの接続（7 ページ）
- ケーブル管理（8 ページ）

ケーブル（必要に応じてキーボード、モニタ ケーブルなど）をサーバの背面に接続します。ケーブルを適切に通し、ケーブル ストラップを使用して、ケーブルをしっかりスライド レールに固定します。アプライアンスの背面図については、図 2（3 ページ） 図 2Cisco SNS-3415/3495 アプライアンスの背面図（3 ページ）を参照してください。

ネットワーク インターフェイスの接続

警告：雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

ここでは、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスのイーサネット ポートを接続する方法について説明します。

イーサネット コネクタは、Serial over LAN（SoL）ケーブルをサポートしています。RJ-45 ポートは、標準的なストレートおよびクロス カテゴリ 5 Unshielded Twisted-Pair（UTP）ケーブルをサポートしています。シスコではカテゴリ 5 UTP ケーブルを販売していません。市販のケーブルを使用してください。

ケーブルをアプライアンスのイーサネット ポートに接続するには、次の手順を実行します。

1. アプライアンスの電源がオフになっていることを確認します。
2. ケーブルの一方の端を、アプライアンス上の GigabitEthernet 0 ポートに接続します。
3. 他方の端をネットワークのスイッチに接続します。

イーサネット ポート コネクタ

Cisco SNS 3515 または Cisco SNS-3595 アプライアンスには、6 個の内蔵デュアルポート イーサネット コントローラが搭載されています。これらのコントローラでは 10-Mb/s、100-Mb/s、または 1000-Mb/s ネットワークに接続するためのインターフェイスと全二重（FDX）機能が提供され、イーサネット LAN 上でデータを同時に送受信できます。ACS 5.8.1 は複数の NIC をサポートしています。詳細については、複数のネットワーク インターフェイス コネクタ（9 ページ）を参照してください。

イーサネット ポートにアクセスするには、カテゴリ 3、4、5、5E、または 6 のシールドなしツイストペア（UTP）ケーブルを、アプライアンスの背面にある RJ-45 コネクタに接続します。

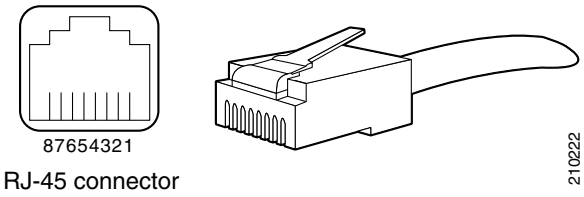
表 1（6 ページ） に、UTP ケーブルのカテゴリを示します。

表 1　イーサネット ケーブル接続ガイドライン

タイプ	説明
10BASE-T	EIA カテゴリ 3、4、または 5 UTP（2 または 4 ペア）、最大 328 フィート（100 m）
100BASE-TX	EIA カテゴリ 5 UTP（2 ペア）、最大 328 フィート（100 m）
1000BASE-T	EIA カテゴリ 6 UTP（推奨）、カテゴリ 5E UTP または 5 UTP（2 ペア）、最大 328 フィート（100 m）

図 6（6 ページ） に、イーサネット RJ-45 ポートとプラグを示します。

図 6　RJ-45 ポートとプラグ



RJ-45 connector

表 2（6 ページ） の一覧では、コネクタで使用される RJ-45 ピン信号について説明します。

表 2　イーサネット ポートのピン配列

イーサネット ポートのピン	信号	説明
1	TxD+	送信データ +
2	TxD-	送信データ -
3	RxD+	受信データ +
4	終端ネットワーク	接続なし
5	終端ネットワーク	接続なし

表 2　イーサネット ポートのピン配列（続き）

イーサネット ポートのピン	信号	説明
6	RxD-	受信データ -
7	終端ネットワーク	接続なし
8	終端ネットワーク	接続なし

コンソールの接続

警告：雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

Cisco SNS-3515 または Cisco SNS-3595 アプライアンスには、コンソール端末をアプライアンスに接続するための DCE モードのコンソール ポートがあります。アプライアンスのコンソール ポートでは、DB-9 シリアル コネクタが使用されています。

Cisco SNS-3515 または Cisco SNS-3595 アプライアンス上のコンソール ポートには、EIA/TIA-232 非同期シリアル（DB-9）コネクタが含まれています。このシリアル コンソール コネクタ（ポート）を使用することで、端末（ターミナル エミュレーション ソフトウェアが動作する PC か ASCII 端末）をコンソール ポートに接続し、アプライアンスにローカルにアクセスできます。

ターミナル エミュレーション ソフトウェアが動作する PC をコンソール ポートに接続するには、両端が DB-9 メスのストレート ケーブルを使用します。

ASCII 端末をコンソール ポートに接続するには、片方が DB-9 メスでもう一方が DB-25 オスのストレート ケーブルと、DB-25 メスから DB-25 メスへの変換アダプタを使用します。

端末またはターミナル エミュレーション ソフトウェアが動作する PC を、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスのコンソール ポートに接続するには、次の手順を実行します。

1. ストレート ケーブルを使用して端末をコンソール ポートに接続します。
2. 端末またはターミナル エミュレーション ソフトウェアを、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、ハードウェア フロー制御なしに設定します。

キーボードとビデオ モニタの接続

警告：雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

ここでは、キーボードとビデオ モニタを Cisco SNS-3515 または Cisco SNS-3595 アプライアンスに接続するための方法について説明します。

Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの前面パネルにある KVM コネクタを使用して、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスにキーボードとビデオ モニタを接続できます。KVM ケーブルは、2 個の USB、1 個の VGA、および 1 個のシリアル コネクタを装備するアプライアンスに同梱されています。

Cisco SNS-3515 または Cisco SNS-3595 アプライアンスはマウスをサポートしていません。

Cisco SNS-3515 または Cisco SNS-3595 には、アプライアンスの背面に USB ポートがあり、キーボードとビデオ モニタを接続するために使用できます。

キーボードとビデオ モニタをアプライアンスに接続するには、次の手順を実行します。

1. アプライアンスの電源がオフになっていることを確認します。
2. キーボード ケーブルの端を、アプライアンスの背面パネルにある PS/2（キーボード）ポートに接続します。
3. ビデオ モニタ ケーブルの端を、アプライアンスの背面パネルにある PS/2（ビデオ モニタ）ポートに接続します。
4. アプライアンスの電源をオンにします。

ケーブル管理

ケーブル管理は、アプライアンスの設定の中で、最も外観に関係する作業です。しかし、ケーブル管理には時間がかかるため、放置しがちです。

今日の装置ラックは、従来よりも多くの装置を収納するようになっています。このため、ラックの内部と外部で整然としたケーブル管理を行う必要性が高まっています。ケーブル管理が適切でないと、ケーブルが損傷したりケーブルの追加や変更に時間がかかったりするだけでなく、重要な通気やアクセスが妨げられます。これらの問題により、装置のパフォーマンスが低下したり、ダウンタイムが長くなったりするおそれがあります。

ケーブル管理を扱うためのソリューションは多数あります。単純なケーブル管理リングから、垂直または水平収納容器、樋やはしごに至るまで、さまざまなソリューションがあります。

すべての Cisco SNS-3515 または Cisco SNS-3595 アプライアンス ケーブルは、ケーブル同士や装置の他の部分と干渉しないように、適切に整理する必要があります。各地の慣習に従って、アプライアンスに接続されているケーブルを適切に整理してください。

設置手順を続行するには、次のセクションCisco SNS-3515 または 3595 アプライアンスの接続と電源投入（8 ページ）に進んでください。

Cisco SNS-3515 または 3595 アプライアンスの接続と電源投入

- サーバの接続と電源投入（スタンドアロン モード）（8 ページ）
- NIC モードおよび NIC 冗長化の設定（12 ページ）
- システム BIOS および CIMC ファームウェア（13 ページ）

サーバの接続と電源投入（スタンドアロン モード）

注: このセクションではサーバの電源投入の方法、IP アドレスの割り当て方法、サーバをスタンドアロン モードで使用する場合のサーバ管理への接続方法について説明します。サーバを Cisco UCS Manager の統合で使用する場合は、特定のケーブル接続および設定が必要です。『Installation for Cisco UCS Integration』を参照してください。

サーバは次のデフォルト設定で出荷されます。

- NIC モードは Shared *LOM EXT* です。

  Shared LOM EXT モードでは、1 Gb イーサネット ポートおよび取り付け済みの Cisco 仮想インターフェイス カード（VIC）上のすべてのポートが、Cisco Integrated Management Interface（Cisco IMC）にアクセスできます。10/100/1000 専用管理ポートを使用して Cisco IMC にアクセスする場合は、次の手順のステップ 1 の説明に従って、サーバに接続して NIC モードを変更できます。

- NIC の冗長性はアクティブ-アクティブです。

  すべてのイーサネット ポートが同時に使用されます。

- DHCP は有効になっています。

- IPv4 は有効になっています。

次の 2 つの方法でシステムに接続することができます。

ローカル設定:キーボードとモニタをシステムに接続して設定を行う場合は、この手順を使用します。この手順では、KVM ケーブル(Cisco PID N20-BKVM)またはサーバの背面にあるポートが使用できます。ローカル接続手順(9 ページ)を参照してください。

リモート設定:専用管理 LAN 経由で設定を行う場合は、この手順を使用します。リモート接続手順(9 ページ)を参照してください。

注:システムをリモートで設定するには、システムと同じネットワーク上に DHCP サーバが存在する必要があります。このサーバ ノードの MAC アドレスの範囲を、DHCP サーバにあらかじめ設定しておく必要があります。MAC アドレスはサーバ ノード背面のラベルに印字されています。このサーバ ノードでは、Cisco IMC に 6 つの MAC アドレスの範囲が割り当てられています。ラベルに印字されている MAC アドレスは、6 つの連続 MAC アドレスのうち最初のものです。

ローカル接続手順

1. 電源コードをサーバの各電源装置に接続し、次に、接地された AC 電源コンセントに各コードを接続します。電源仕様については、電源仕様(5 ページ)を参照してください。

   最初のブートアップ中、サーバがスタンバイ電源でブートするまでに約 2 分かかります。

   システムの電源ステータスは、前面パネルのシステムの電源ステータス LED で確認できます(Cisco SNS 3515 および 3595 アプライアンスの LED インジケータ(6 ページ)を参照)。LED がオレンジの場合、サーバはスタンバイ電源モードです。

2. 次のいずれかの方法を使用して、USB キーボードと VGA モニタをサーバに接続します。

- USB キーボードと VGA モニタを背面パネルの対応するコネクタに接続します(Cisco SNS-3515 および Cisco SNS-3595 アプライアンスの概要(1 ページ)を参照)。
- オプションの KVM ケーブル(Cisco PID N20-BKVM)を前面パネルの KVM コネクタに接続します(コネクタの位置については、Cisco SNS-3515 および Cisco SNS-3595 アプライアンスの概要(1 ページ)を参照)。USB キーボードと VGA モニタを KVM ケーブルに接続します。

3. Cisco IMC 設定ユーティリティを開きます。

   a. a. 前面パネルの電源ボタンを 4 秒間長押しして、サーバを起動します。

   b. b. ブートアップ時に、Cisco IMC 設定ユーティリティを開くよう求められたら F8 を押します。

   このユーティリティには 2 つのウィンドウがあり、F1 または F2 を押すことで切り替えることができます。

4. Cisco IMC 設定ユーティリティのセットアップ(10 ページ)に進みます。

リモート接続手順

1. 電源コードをサーバの各電源装置に接続し、次に、接地された AC 電源コンセントに各コードを接続します。電源仕様については、電源仕様(5 ページ)を参照してください。

   最初のブートアップ中、サーバがスタンバイ電源でブートするまでに約 2 分かかります。

   システムの電源ステータスは、前面パネルのシステムの電源ステータス LED で確認できます(Cisco SNS 3515 および 3595 アプライアンスの LED インジケータ(6 ページ)を参照)。LED がオレンジの場合、サーバはスタンバイ電源モードです。

2. 管理イーサネット ケーブルを背面パネルの専用管理ポートに差し込みます(Cisco SNS-3515 および Cisco SNS-3595 アプライアンスの概要(1 ページ)を参照)。

3. 事前設定された DHCP サーバで、サーバ ノードに IP アドレスを割り当てられるようにします。
4. 割り当てられた IP アドレスを使用して、サーバ ノードの Cisco IMC にアクセスし、ログインします。IP アドレスを特定するには、DHCP サーバの管理者に相談してください。

   注：サーバのデフォルトのユーザ名は admin です。デフォルト パスワードは password です。
5. Cisco IMC サーバの [Summary] ページで、[Launch KVM Console] をクリックします。別の KVM コンソール ウィンドウが開きます。
6. Cisco IMC の [Summary] ページで、[Power Cycle Server] をクリックします。システムがリブートします。
7. KVM コンソール ウィンドウを選択します。

   注：次のキーボード操作を有効にするには、KVM コンソール ウィンドウがアクティブ ウィンドウである必要があります。
8. プロンプトが表示されたら、F8 を押して、Cisco IMC 設定ユーティリティを起動します。このユーティリティは、KVM コンソール ウィンドウで開きます。

   このユーティリティには 2 つのウィンドウがあり、F1 または F2 を押すことで切り替えることができます。
9. Cisco IMC 設定ユーティリティのセットアップ（10 ページ）に進みます。

Cisco Integrated Management Controller（CIMC）

組み込みの Cisco Integrated Management Controller 1.4.7a（CIMC）GUI または CLI インターフェイスを使用して、サーバ インベントリ、状態、およびシステム イベント ログをモニタできます。次の URL で、使用しているファームウェア リリースのユーザ マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

Cisco IMC 設定ユーティリティのセットアップ

システムに接続して Cisco IMC 設定ユーティリティを開いた後に、次の手順を実行します。

1. NIC モードと NIC 冗長性を設定します。

   a. a. NIC モードを設定して、サーバ管理で Cisco IMC にアクセスする際に使用するポートを選択します（ポートの識別については、図 1-3 を参照）。

- [Shared LOM EXT]（デフォルト）：これは、工場出荷時設定の Shared LOM 拡張モードです。このモードでは、Shared LOM インターフェイスと Cisco Card インターフェイスの両方がイネーブルです。

  このモードでは、DHCP 応答が Shared LOM ポートと Cisco カード ポートの両方に返されます。サーバがスタンドアロン モードであるために、Cisco カード接続でその IP アドレスが Cisco UCS Manager システムから取得されないと判別された場合は、その Cisco カードからのその後の DHCP 要求はディセーブルになります。スタンドアロン モードで Cisco カードを介して Cisco IMC に接続する場合は、Cisco Card NIC モードを使用します。
- [Shared LOM]：Cisco IMC へのアクセスに 1 Gb イーサネット ポートを使用します。NIC 冗長化と IP 設定を選択する必要があります。
- [Dedlicated]：Cisco IMC へのアクセスに専用管理ポートを使用します。NIC 冗長化と IP 設定を選択する必要があります。
- [Cisco Card]：Cisco IMC へのアクセスに取り付け済みの Cisco UCS 仮想インターフェイス カード（VIC）のポートを使用します。NIC 冗長化と IP 設定を選択する必要があります。

  必須の VIC スロットの設定も下記で参照してください。

- [VIC Slot]：Cisco Card NIC モードを使用する場合、VIC を取り付けた場所に合わせて、この設定を選択する必要があります。Riser1、Riser2、または Flex-LOM（mLOM スロット）のいずれかを選択します。
  - Riser1 を選択する場合、スロット 1 が使用されます。
  - Riser2 を選択する場合、スロット 2 が使用されます。
  - Flex-LOM を選択する場合、mLOM スロットで mLOM-style VIC を使用する必要があります。

  b. b. 必要に応じて NIC 冗長化を変更するには、このユーティリティを使用します。このサーバでは、次の 3 つの NIC 冗長化設定を行うことができます。

- [None]：イーサネット ポートは個別に動作し、問題が発生した場合にフェールオーバーを行いません。この設定は、専用 NIC モードでのみ使用できます。
- [Active-standby]：アクティブなイーサネット ポートに障害が発生した場合、スタンバイ ポートにトラフィックがフェールオーバーします。
- [Active-active]：すべてのイーサネット ポートが同時に使用されます。Shared LOM EXT モードでは、この NIC 冗長化の設定のみが可能です。Shared LOM と Cisco Card モードでは、アクティブ-スタンバイとアクティブ-アクティブの両方の設定が使用可能です。

2. ダイナミック ネットワーク設定用に DHCP をイネーブルにするか、スタティック ネットワーク設定を入力するかを選択します。

注：DHCP をイネーブルにするには、DHCP サーバにこのサーバの MAC アドレスの範囲をあらかじめ設定しておく必要があります。MAC アドレスはサーバ背面のラベルに印字されています。このサーバでは、Cisco IMC に 6 つの MAC アドレスの範囲が割り当てられています。ラベルに印字されている MAC アドレスは、6 つの連続 MAC アドレスのうち最初のものです。

スタティック IPv4 および IPv6 設定には次が含まれます。

- Cisco IMC の IP アドレス。
- プレフィックス/サブネット。

  IPv6 の場合、有効な値は 1 ～ 127 です。
- ゲートウェイ。

  IPv6 の場合、ゲートウェイが不明な場合は、::（コロン 2 つ）を入力して none のままに設定することができます。
- 優先 DNS サーバ アドレス。

  IPv6 の場合、::（コロン 2 つ）を入力してこれを none のままに設定することができます。

3. （任意）このユーティリティを使用して、VLAN 設定を行います。
4. F1 を押して 2 番目の設定ウィンドウに移動したら、次のステップに進みます。

   2 番目のウィンドウで F2 を押すと、最初のウィンドウに戻ることができます。
5. （任意）サーバのホスト名を設定します。
6. （任意）ダイナミック DNS をイネーブルにし、ダイナミック DNS（DDNS）ドメインを設定します。
7. （任意）[Factory Default] チェックボックスをオンにすると、サーバは出荷時の初期状態に戻ります。
8. （任意）デフォルトのユーザ パスワードを設定します。
9. （任意）ポート設定の自動ネゴシエーションをイネーブルにするか、ポート速度およびデュプレックス モードを手動で設定します。

注：自動ネゴシエーションは専用 NIC モードを使用する場合にのみ使用できます。自動ネゴシエーションはサーバが接続されているスイッチ ポートに基づいて自動的にポート速度およびデュプレックス モードを設定します。自動ネゴシエーションをディセーブルにした場合、ポート速度およびデュプレックス モードを手動で設定する必要があります。

10. （任意）ポート プロファイルとポート名をリセットします。
11. **F5** を押して、設定した内容に更新します。新しい設定が表示され、メッセージ「Network settings configured」が表示されるまでに約 45 秒かかる場合があります。その後、次の手順でサーバを再起動します。
12. F10 を押して設定を保存し、サーバをリブートします。

注：DHCP を有効にすると、ブートアップの間、動的に割り当てられた IP アドレスと MAC アドレスがコンソール画面に表示されます。

ブラウザと Cisco IMC の IP アドレスを使用して、Cisco IMC 管理インターフェイスに接続します。IP アドレスは、行った設定に基づいています（スタティック アドレスまたは DHCP サーバによって割り当てられたアドレス）。

注：サーバのデフォルトのユーザ名は admin です。デフォルト パスワードは password です。

サーバを管理するには、これらのインターフェイスの使用手順について『Cisco UCS C-Series Rack-Mount Server Configuration Guide』または『Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide』を参照してください。これらのマニュアルへのリンクは、次の URL の C シリーズ マニュアル ロードマップ内にあります。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

NIC モードおよび NIC 冗長化の設定

NIC モード

このサーバには、次のような選択可能な NIC モード設定があります。

- [Shared LOM EXT]（デフォルト）：これは、工場出荷時設定の Shared LOM 拡張モードです。このモードでは、Shared LOM インターフェイスと Cisco Card インターフェイスの両方がイネーブルです。

  このモードでは、DHCP 応答が Shared LOM ポートと Cisco カード ポートの両方に返されます。サーバがスタンドアロン モードであるために、Cisco カード接続でその IP アドレスが Cisco UCS Manager システムから取得されないと判別された場合は、その Cisco カードからのその後の DHCP 要求はディセーブルになります。Cisco カード接続でその IP アドレスが Cisco UCS Manager システムから取得されると判別された場合、応答にはサーバを自動的に UCSM モードにするパラメータが含まれます。
- [Dedicated]：Cisco IMC へのアクセスに専用管理ポートを使用します。NIC 冗長化と IP 設定を選択する必要があります。
- [Shared LOM]：Cisco IMC へのアクセスに 1 Gb イーサネット ポートを使用します。NIC 冗長化と IP 設定を選択する必要があります。
- [Cisco Card]：Cisco IMC へのアクセスに取り付け済みの Cisco UCS 仮想インターフェイス カード（VIC）のポートを使用します。NIC 冗長化と IP 設定を選択する必要があります。

  必須の VIC スロットの設定も下記で参照してください。
- [VIC Slot]：Cisco Card NIC モードを使用する場合、VIC を取り付けた場所に合わせて、この設定を選択します。Riser1、Riser2、または Flex-LOM（mLOM スロット）のいずれかを選択します。
  - Riser1 を選択する場合、スロット 1 が使用されます。
  - Riser2 を選択する場合、スロット 2 が使用されます。
  - Flex-LOM を選択する場合、mLOM スロットで mLOM-style VIC を使用する必要があります。

NIC 冗長化

このサーバには、次のような選択可能な NIC 冗長化設定があります。

- [None]：イーサネット ポートは個別に動作し、問題が発生した場合にフェールオーバーを行いません。この設定は、専用 NIC モードでのみ使用できます。
- [Active-standby]：アクティブなイーサネット ポートに障害が発生した場合、スタンバイ ポートにトラフィックがフェールオーバーします。
- [Active-active]：すべてのイーサネット ポートが同時に使用されます。Shared LOM EXT モードでは、この NIC 冗長化の設定のみが可能です。Shared LOM と Cisco Card モードでは、アクティブ-スタンバイとアクティブ-アクティブの両方の設定が使用可能です。

  アクティブ-アクティブ設定では、モード 5 またはバランス TLB（ロード バランシングを発信する適応型）を使用します。これは特別なスイッチのサポートを必要としないチャネル ボンディングです。発信トラフィックは、各スレーブの現在の負荷（速度に関連して計算される）に応じて分散されます。着信トラフィックは現在のスレーブによって受信されます。受信スレーブで障害が発生すると、障害が発生した受信スレーブの MAC アドレスを別のスレーブが引き継ぎます。

システム BIOS および CIMC ファームウェア

ここでは、システム BIOS 1.4.7b.0 について説明します。この項の内容は次のとおりです。

- BIOS および Cisco IMC ファームウェアの更新（13 ページ）
- システム BIOS へのアクセス（14 ページ）

BIOS および Cisco IMC ファームウェアの更新

注意：BIOS ファームウェアを更新する際には CIMC ファームウェアも同一のバージョンにアップグレードする必要があります。そうしないと、サーバが起動しません。BIOS と CIMC のファームウェアが一致するまで電源をオフにしないでください。オフにすると、サーバが起動しません。
シスコは、BIOS、CIMC、およびその他のファームウェアを互換性のあるレベルに同時にアップグレードできるよう支援するために、Cisco Host Upgrade Utility を提供しています。

サーバには、シスコが提供し、承認しているファームウェアが使用されています。シスコは、各ファームウェア イメージと共にリリース ノートを提供しています。ファームウェアを更新するには、いくつかの方法があります。

- **ファームウェア レベル 1.2 以降を実行するシステムの場合の推奨方法**：Cisco Host Upgrade Utility を使用して、CIMC 1.4.7a、BIOS 1.4.7b.0、LOM、LSI ストレージ コントローラ、および Cisco UCS P81E VIC ファームウェアを同時に互換性のあるレベルにアップグレードします。

ファームウェア レベルについては、下記のマニュアル ロードマップ リンクにある『*Cisco Host Upgrade Utility Quick Reference Guide*』を参照してください。

注：Cisco Host Upgrade Utility を使用するには、システム ファームウェアがレベル 1.2 以降である必要があります。ファームウェアがレベル 1.2 よりも前のレベルである場合は、次の方法で BIOS および CIMC ファームウェアを個別に更新する必要があります。

- EFI インターフェイスを使用して BIOS をアップグレードするか、Windows または Linux プラットフォームからアップグレードすることができます。『Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide』を参照してください。
- CIMC GUI インターフェイスを使用して CIMC と BIOS のファームウェアをアップグレードできます。『Cisco UCS C-Series Rack-Mount Server Configuration Guide』を参照してください。
- CIMC CLI インターフェイスを使用して CIMC と BIOS のファームウェアをアップグレードできます。『Cisco UCS C-Series Rack-Mount Server CLI Configuration Guide』を参照してください。

上記のマニュアルへのリンクについては、次の URL にあるマニュアル ロードマップを参照してください。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

システム BIOS へのアクセス

サーバの BIOS 設定を変更するには、次の手順に従います。詳しい手順は、BIOS 画面にも表示されます。

1. ブートアップ時にメッセージが表示されたら、F2 キーを押して BIOS セットアップ ユーティリティに切り替えます。

   注：現在の BIOS のバージョンとビルドはユーティリティの [Main] ページに表示されます。

2. 矢印キーを使って、BIOS メニュー ページを選択します。
3. 矢印キーを使って、変更するフィールドを反転表示にします。
4. Enter を押して変更するフィールドを選択し、そのフィールドの値を変更します。
5. [Exit] メニュー画面が表示されるまで右矢印キーを押します。
6. [Exit] メニュー画面の指示に従って変更内容を保存し、セットアップ ユーティリティを終了します（または、F10 を押します）。Esc を押すと、変更内容を保存せずにユーティリティを終了できます。

Cisco SNS-3515 および Cisco SNS-3595 を使用した Secure Access Control System のインストールと設定

この章では、Cisco SNS-3515 または Cisco SNS-3595 と ACS 5.8.1 サーバのインストールおよび初期設定の方法について説明します。

この章の内容は、次のとおりです。

- Cisco SNS-3515/3595 アプライアンスへの ACS のインストール（1 ページ）
- Cisco Secure ACS 5.8.1 ISO イメージのダウンロード（2 ページ）
- ACS サーバのインストール（2 ページ）
- 管理者パスワードのリセット（9 ページ）
- Cisco SNS-3515/3595 アプライアンスのイメージの再作成（10 ページ）

Cisco SNS-3515/3595 アプライアンスへの ACS のインストール

Cisco SNS-3515 または Cisco SNS-3595 アプライアンスには、ACS 5.8.1 ソフトウェアがあらかじめインストールされています。ここでは、インストール プロセスの概要と、ACS をインストールする前に実行する必要がある作業について説明します。

ACS 5.8.1 のインストールを開始する前に、次の作業を実行する必要があります。

1. 箱を開けて内容を確認します。サーバの開梱と点検（2 ページ）を参照してください
2. Cisco SNS-3415 および Cisco SNS-3495 ハードウェア アプライアンスの導入（1 ページ）を参照してください。
3. Cisco SNS 3415 および Cisco SNS 3495 ハードウェア アプライアンスの設置の準備（1 ページ）にある、一般的な注意事項と安全に関する警告を読みます。
4. アプライアンスをラックに取り付けます。サーバの設置準備（3 ページ）を参照してください
5. Cisco SNS-3515 または Cisco SNS-3595 をネットワークとアプライアンス コンソールに接続します。ケーブルの接続（7 ページ）を参照してください
6. Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの電源をオンにします。Cisco SNS-3415/3495 アプライアンスの接続と電源投入（10 ページ）を参照してください
7. ネットワークとアプライアンス コンソールに対して、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの電源をオンにします。ケーブルの接続（7 ページ）を参照してください
8. CLI プロンプトで **setup** コマンドを実行し、ACS サーバの初期設定を行います。セットアップ プログラムの実行（5 ページ）を参照してください。アプライアンス コンソールまたは CIMC を使用して、設定を行うことができます。

『Cisco UCS Server Configuration Utility, Release 3.0 User Guide』ガイドを使用して、Cisco SNS-3515 アプライアンスまたは Cisco SNS-3595 アプライアンスを設定できます。Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの詳細については、『Cisco UCS C-Series Rack Server guides』も参照できます。

Cisco Secure ACS 5.8.1 ISO イメージのダウンロード

Cisco.com から Cisco Secure ACS 5.8.1 ISO イメージをダウンロードできます。

1. http://www.cisco.com/go/acs にアクセスします。このリンクにアクセスするには、有効な Cisco.com ログイン クレデンシャルを所有している必要があります。
2. [Download Software] をクリックします。

Cisco.com ページに Cisco Secure ACS リリース 5.8.1 ソフトウェア イメージが表示されます。インストールおよび初期設定が完了したら、すべての Cisco ACS サービスのテストを実行できます。

注:ACS 5.x ソフトウェア イメージを Cisco.com からダウンロードできるのは、以前のバージョンの ACS 5.x ソフトウェアについて有効な Software Application Support(SAS)契約を結んでいる場合だけです。以前のバージョンで有効な SAS 契約を結んでいない場合は、Cisco.com のソフトウェア イメージを特定のカスタマー アカウントに公開するには、販売エンジニア(SE)、アカウント マネージャ(AM)、またはシスコ パートナーにお問い合わせください。

ACS サーバのインストール

Cisco Secure ACS 5.8.1 ISO イメージをダウンロードしたら、次のいずれかのオプションを使用して、アプライアンスに Cisco Secure ACS 5.8 ソフトウェアをインストールおよび設定できます。

- Cisco Integrated Management Interface(CIMC)を設定し、CIMC を使用して、ネットワークを介してリモートから Cisco Secure ACS 5.8.1 をインストールします。CIMC の設定(5 ページ)、CIMC を使用したリモートからの Cisco SNS-3515/3595 アプライアンスへの ACS 5.8.1 のインストール(2 ページ)、およびセットアップ プログラムの実行(5 ページ)を参照してください。
- ブート可能な USB ドライブを作成し、USB ドライブを使用して、Cisco Secure ACS 5.8.1 をインストールします。ブート可能な USB ドライブの作成(4 ページ)、USB ドライブを使用した Cisco SNS-3515/3595 アプライアンスへの ACS 5.8.1 のインストール(4 ページ)、およびセットアップ プログラムの実行(5 ページ)を参照してください。

CIMC を使用したリモートからの Cisco SNS-3515/3595 アプライアンスへの ACS 5.8.1 のインストール

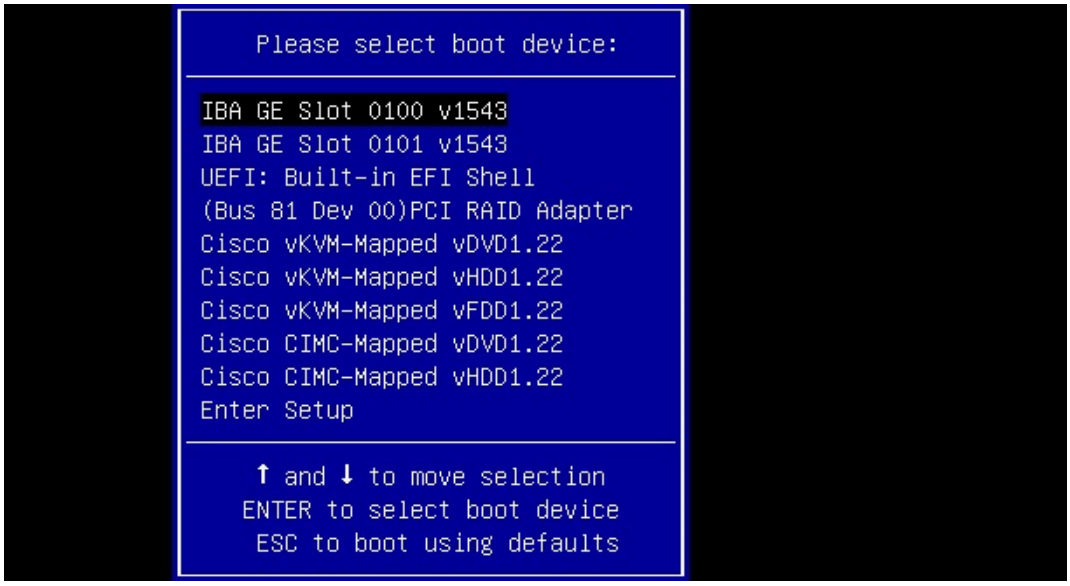
アプライアンスの CIMC を設定したら、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの管理に使用できます。CIMC を通じて、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスで BIOS 設定を含むすべての操作を実行できます。

1. サーバ管理用の CIMC に接続します。NIC モードの設定で選択したポートを使用して、LAN からサーバにイーサネット ケーブルを接続します。[Active-active] および [Active-passive] の [NIC redundancy] 設定では、2 つのポートに接続する必要があります。
2. ブラウザと CIMC の IP アドレスを使用して CIMC セットアップ ユーティリティにログインします。IP アドレスは、設定した CIMC に基づいています(スタティック アドレスまたは DHCP サーバによって割り当てられたアドレス)。

   注:サーバのデフォルトのユーザ名は *admin* です。デフォルト パスワードは *password* です。
3. CIMC クレデンシャルを使用してログインします。
4. [Launch KVM Console] をクリックします。
5. [Virtual Media] をクリックします。
6. 一覧から、[Activate Virtual Devices] を選択します。

   [Activate Virtual Devices] オプション近くのチェックマークが表示されます。
7. [Virtual Media] を再度クリックし、[MAP CD/DVD] オプションを選択します。

8. [Browse] をクリックして ACS 5.8.1 ISO イメージを探します。
9. [Map Device] をクリックします。
10. [Macros] > [Static Macros] > [Ctrl-Alt-Del] の順に選択して、ISO イメージを使用して Cisco SNS-3515 または Cisco SNS-3595 アプライアンスを起動します。
11. F6 キーを押して、ブート メニューを起動します。次のような画面が表示されます。



12. CD/DVD にマッピングした Cisco vKVM-Mapped vDVD を選択して、Enter キーを押します。次のメッセージが表示されます。

```
Welcome to the Cisco Secure ACS 5.8.1 Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS Installation (Keyboard/Monitor)
[2] Cisco Secure ACS Installation (Serial Console)
[3] Recover administrator password (Keyboard/Monitor
[4] Recover administrator password (Serial Console)
<Enter> Boot existing OS from hard disk.
Enter boot option and press <Enter>
boot:
```

13. ブート プロンプトで、1 を入力して、Enter キーを押します。
14. セットアップ モードでネットワーク設定パラメータを入力すると、アプライアンスが自動的に再起動し、シェル プロンプト モードに戻ります。
15. シェル プロンプト モードを終了します。アプライアンスが起動します。
16. インストール プロセスの確認（5 ページ）に進みます。

USB ドライブを使用した Cisco SNS-3515/3595 アプライアンスへの ACS 5.8.1 のインストール

USB ドライブを使用して Cisco SNS-3515 または Cisco SNS-3595 アプライアンスに ACS 5.8.1 をインストールするには、次の手順を実行します。

はじめる前に

ブート可能な USB ドライブを作成する必要があります。ブート可能な USB ドライブの作成（4 ページ）を参照してください。

1. Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの電源をオンにします。
2. Cisco Secure ACS ISO イメージを持つブート可能な USB ドライブを USB ポートに差し込みます。
3. ACS を再起動して、BIOS モードに進みます。
4. BIOS モードでは、USB からのブートを選択します。
5. BIOS モードを終了して、[Save] をクリックします。
6. 再び ACS を再起動し、USB から起動します。
7. ここで、USB ドライブを使用して、Cisco SNS-3515 または Cisco SNS-3595 のイメージの再作成を続けます。

   次のメッセージが表示されます。

```
Welcome to the Cisco Secure ACS 5.8.1 Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS Installation (Keyboard/Monitor)
[2] Cisco Secure ACS Installation (Serial Console)
[3] Reset administrator password (Keyboard/Monitor
[4] Reset administrator password (Serial Console)
<Remove USB key and reboot to boot existing Hard Disk>
Please enter boot option and press <Enter>
boot:
```

8. ブート プロンプトで、**1** を入力して、Enter キーを押します。
9. セットアップ モードでネットワーク設定パラメータを入力すると、アプライアンスが自動的に再起動し、シェル プロンプト モードに戻ります。
10. シェル プロンプト モードを終了します。アプライアンスが起動します。
11. インストール プロセスの確認（5 ページ）に進みます。

ブート可能な USB ドライブの作成

SNS-3515 と SNS-3595 用の ACS 5.8.1 USB インストールツール（*ACS_58_USB_Installation_tool.zip*）は、Cisco.com で、Cisco Secure ACS 5.8.1 の Download Software セクションからダウンロードできます。この zip ファイルにはブート可能なスクリプトが含まれ、これを抽出すると Cisco Secure Access Control System 5.8.1 をインストールするためにブート可能な USB を作成できます。

はじめる前に

- *ACS_581_USB_Installation_tool.zip* ファイルが必要です。
- 次の項目が必要になります。
  - RHEL-5 または RHEL-6 Linux マシン、CentOS 5.*x* または CentOS 6.*x*。PC または MAC を使用する場合は、Linux VM がインストールされていることを確認してください。

- 4 GB の USB ドライブ
- iso-to-usb.sh スクリプト

■ ローカル Linux マシンのドライブへのアクセス権限が必要です。

1. USB ポートに USB ドライブを差し込みます。
2. Linux マシンのディレクトリに iso-to-usb.sh スクリプトと Cisco Secure ACS 5.8.1 ISO イメージをコピーします。
3. 次のコマンドを入力します。

   iso-to-usb.sh source_iso usb_device

   たとえば、# **./iso-to-usb.sh** *ACS_v5.8.1.0.22.iso/dev/sdc* では、**iso-to-usb.sh** はスクリプトの名前で、*ACS_v5.8.1.0.22.iso* は ISO イメージの名前で、*/dev/sdc* は USB デバイスです。

   成功したことを示す、次のメッセージが表示されます。

```
*** W A R N I N G ***
THIS SCRIPT WILL DELETE ALL EXISTING CONTENT ON YOUR USB DRIVE: /dev/sdb/
ARE YOU SURE YOU WANT TO CONTINUE? [Y/N]: y
Deleting partition table on USB drive: /dev/sdb...
Creating new partition table on USB drive: /dev/sdb...
Formatting BOOT partition: /dev/sdb1 as VFAT...
Formatting DATA partition: /dev/sdb2 as EXT2...
Copying syslinux files to USB partition: /dev/sdb1...
Copying ISO file to USB partition: /dev/sdb2...
DONE!
```

4. USB ドライブを外します。

注:**iso-to-usb.sh** コマンドを実行した後、USB ドライブは非 Linux オペレーティング システムが使用できるすべての領域を認識しない形式でパーティション化されます。Windows または MAC オペレーティング システムとの一般的な使用に対して USB ドライブを再パーティション化するには、このディレクトリでコマンドの **repurpose-usb.sh** ユーティリティを実行する必要があります。このユーティリティは再パーティション化され、一般的な使用に対して USB キーを再フォーマットします。

セットアップ プログラムの実行

ここでは、ACS サーバをインストールするためのセットアップ プロセスについて説明します。

セットアップ プログラムでは、必要なパラメータの入力を求める、対話型のコマンドライン インターフェイス（CLI）が起動されます。

管理者は、コンソールまたはダム端末とセットアップ プログラムを使用して、ACS 5.8.1 サーバの初期ネットワークを設定し、初期管理者資格情報を設定します。セットアップ プロセスは一度だけ実行する設定作業です。

ACS サーバをインストールするには、次の手順を実行します。

1. アプライアンスの電源をオンにします。

   次のセットアップ プロンプトが表示されます。

```
Please type 'setup' to configure the appliance
localhost login:
```

2. ログイン プロンプトで **setup** と入力し、Enter を押します。

   コンソールにパラメータのセットが表示されます。表 1（6 ページ）の説明に従ってパラメータを入力します。

注: セットアップ プロセスは、最後のセットアップ値を入力する前に、Ctrl+C を押すことでいつでも中断できます。

表 1　ネットワーク設定パラメータ

プロンプト	デフォルト	条件	説明
ホスト名	*localhost*	最初の文字は ASCII 文字である必要があります。 長さは 3 ～ 15 文字である必要があります。 有効な文字は、英数字（A ～ Z、a ～ z、0 ～ 9）とハイフン（-）で、最初の文字はアルファベットである必要があります。 **注:** AD ID ストアを使用し、同じ名前のプレフィックスで複数の ACS インスタンスを設定する場合は、ホスト名として最大 15 文字を使用して AD 機能が影響を受けないようにします。	ホスト名を入力します。
IPV4 IP Address	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	IP アドレスを入力します。
IPv4 Netmask	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なネットマスクを入力します。
IPv4 Gateway	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なデフォルト ゲートウェイを入力します。
ドメイン名	なし。ネットワーク固有	IP アドレスは入力できません。 有効な文字は、ASCII 文字、数値、ハイフン（-）、およびピリオド（.）です。	ドメイン名を入力します。
IPv4 Primary Name Server Address	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。	有効なネーム サーバ アドレスを入力します。
Add/ another nameserver	なし。ネットワーク固有	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレスにする必要があります。 **注:** ACS CLI から最大 3 つのネーム サーバを設定できます。	複数のネーム サーバを設定するには、**y** と入力します。
NTP サーバ	time.nist.gov	0.0.0.0 ～ 255.255.255.255 の範囲の有効な IPv4 アドレス、またはドメイン ネーム サーバにする必要があります。 **注:** ACS CLI から最大 3 つの NTP サーバを設定できます。	有効なドメイン ネーム サーバまたは IPv4 アドレスを入力します。
タイムゾーン	UTC	有効なローカル タイム ゾーンである必要があります。	有効なタイム ゾーンを入力します。
SSH サービス	なし。ネットワーク固有	なし	SSH サービスを有効にするには、**y** と入力します。

表 1　ネットワーク設定パラメータ（続き）

プロンプト	デフォルト	条件	説明
ユーザ名	admin	最初の管理ユーザの名前です。デフォルトを受け入れるか、新しいユーザ名を入力します。 ユーザ名は 3 ～ 8 文字の英数字（A ～ Z、a ～ z、0 ～ 9）にする必要があります。	ユーザ名を入力します。
Admin パスワード	なし	デフォルトのパスワードはありません。パスワードを入力します。 パスワードは最低 6 文字で、小文字、大文字、数字がそれぞれ 1 つ以上含まれている必要があります。 また、次の点に注意してください。 ■ 初期設定で設定したアカウントのユーザとパスワードの情報は大切に保管してください。 ■ これらのクレデンシャルを使用すると、ACS ハードウェア、CLI、アプリケーションを管理者として完全に制御できるため、忘れないようにして保護します。 ■ 管理者のクレデンシャルを紛失した場合、ACS 5.8.1 のインストール CD を使用してパスワードをリセットできます。	パスワードを入力します。

コンソールで、次のパラメータを入力するよう求められます。

```
localhost login: setup
Enter hostname[]: acs-server-1
Enter IP address[]: a.b.c.d
Enter IP default netmask[]: 255.255.255.255
Enter IP default gateway[]: a.b.c.d
Enter default DNS domain[]: mycompany.com
Enter primary nameserver[]: a.b.c.d
Add secondary nameserver? Y/N : n
Add primary NTP server [time.nist.gov]: a.b.c.d
Add secondary NTP server? Y/N : n
Enter system timezone[UTC]:
Enable SSH service Y/N [N] : y
Enter username [admin]: admin
Enter password:
Enter password again:
Pinging the gateway...
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing acs...
Generating configuration...
Rebooting...
```

ACS サーバのインストールが完了すると、システムは自動的に再起動します。

この時点で、セットアップ プロセスで設定した CLI ユーザ名とパスワードを使用して ACS にログインできるようになります。

注: このユーザ名とパスワードを使用して ACS にログインできるのは、CLI を通じてだけです。

注: ACS 5.8.1 の初期設定では、サーバに IPv4 IP アドレスを設定する必要があります。サーバの IPv6 IP アドレスは、初期設定完了後にのみ設定できます。

注: ACS 5.8.1 は、IPv4 と IPv6 のデュアル スタック ネットワーキングをサポートしていますが、純粋な IPv6 ネットワークはサポートしていません。

インストール プロセスの確認

インストール プロセスが正しく完了したことを確認するには、次の手順を実行します。

1. システムが再起動したら、ログイン プロンプトでセットアップ時に設定したユーザ名を入力し、Enter を押します。
2. パスワード プロンプトで、セットアップ時に設定したパスワードを入力し、Enter を押します。
3. アプリケーションが適切にインストールされていることを確認するために、**show application** コマンドを入力し、**Enter** を押します。

   コンソールに次のメッセージが表示されます。

```
<name>          <Description>
acs Cisco Secure Access Control System 5.8.1
```

4. システム プロンプトでインストールされているリリースと ACS のバージョンを確認するため、**show application version acs** コマンドを入力して Enter を押します。

   コンソールに次のメッセージが表示されます。

```
Cisco ACS VERSION INFORMATION

-----------------------------

Version : 5.8.1.4
Internal Build ID : B.462
```

注: このリリースの別のバージョンでは、Version と Internal Build ID が変更されている場合があります。

5. ACS プロセスのステータスを確認するために、システム プロンプトで **show application status acs** と入力し、**Enter** を押します。

   コンソールに次のメッセージが表示されます。

```
ACS role: PRIMARY
Process 'database'                running
Process 'management'              running
Process 'runtime'                 running
Process 'adclient'                running
Process 'ntpd'                    running
Process 'view-database'           running
Process 'view-jobmanager'         running
Process 'view-alertmanager'       running
Process 'view-collector'          running
Process 'view-logprocessor'       running
```

注: 最新の ACS パッチを入手し ACS を最新に保つには、http://software.cisco.com/download/navigator.html?i=rt を参照してください。

管理者パスワードのリセット

管理者パスワードを失ったためにシステムにログインできない場合は、ACS 5.8.1 Recovery DVD を使用して管理者パスワードをリセットできます。

注: ブート可能な USB ドライブと CIMC を使用して、管理者のパスワードをリセットすることもできます。

管理者パスワードをリセットするには、次の手順を実行します。

1. アプライアンスの電源をオンにします。
2. ACS 5.8.1 Recovery DVD を挿入します。

   コンソールに次のメッセージが表示されます。

```
Welcome to Cisco Secure ACS 5.8.1 Recovery
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS 5.8.1 Installation (Keyboard/Monitor)
[2] Cisco Secure ACS 5.8.1 Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot:
```

   管理者パスワードをリセットするには、システム プロンプトで、キーボードとビデオ モニタを使用している場合は **3** と入力し、シリアル コンソール ポートを使用している場合は **4** と入力します。

   コンソールにパラメータのセットが表示されます。

3. 表 2（9 ページ）の説明に従ってパラメータを入力します。

表 2　パスワード リセット パラメータ

パラメータ	説明
Admin username	パスワードをリセットする管理者の番号を入力します。
Password	管理者の新しいパスワードを入力します。
Verify password	パスワードを再度入力します。
Save change & Reboot	保存するには **y** と入力します。

   コンソールに次のメッセージが表示されます。

```
Admin username:
[1]:admin
[2]:admin2
[3]:admin3
Enter number of admin for password recovery:1
Password
Verify password:
Save change&reeboot? [Y/N]:
```

Cisco SNS-3515/3595 アプライアンスのイメージの再作成

CIMC またはブート可能な USB ドライブを使用して、ACS 5.8.1 を使用した Cisco SNS-3515 または Cisco SNS-3595 アプライアンスのイメージを再作成できます。

Cisco SNS-3515 または Cisco SNS-3595 アプライアンスのイメージを再作成するには、次の手順を実行します。

- CIMC を使用してイメージを再作成します。CIMC を使用したリモートからの Cisco SNS-3515/3595 アプライアンスへの ACS 5.8.1 のインストール（2 ページ）を参照してください
- ブート可能な USB ドライブを使用して、イメージを再作成します。USB ドライブを使用した Cisco SNS-3515/3595 アプライアンスへの ACS 5.8.1 のインストール（4 ページ）を参照してください

法規制の遵守

法令準拠および安全性に関する情報については、『*Regulatory Compliance and Safety Information for Cisco Secure Access Control System*』を参照してください。

VMware 仮想マシン上の ACS 5.8.1

VMware 仮想マシンへの ACS のインストール

この章では、ACS 5.8.1 のシステム要件と VMware 仮想マシンへのインストールについて説明します。

ここでは、次の項目について説明します。

- 仮想マシン要件（1 ページ）
- ESXi 5.5 および ESXi 6.0 用 VM の設定（4 ページ）
- ACS サーバをインストールするための VM の準備（9 ページ）
- ESXi 5.5 および 6.0 での ACS サーバのインストール（10 ページ）
- VMWare 強化の要件（12 ページ）
- VMware ツールのサポート（12 ページ）

仮想マシン要件

VMware 仮想マシン（VM）の最小システム要件は、CSACS-1121 アプライアンスのハードウェア構成と同様です。

表 1（1 ページ）に、VMware 仮想マシンに ACS 5.8.1 をインストールするための最小システム要件を示します。

表 1　　最小システム要件

要件のタイプ	最小要件
CPU	■ 2 個の CPU（デュアル CPU、Xeon、Core2 Duo、または 2 個のシングル CPU） ■ 2GHz CPU 速度
メモリ	4 GB RAM
ハード ディスク	最小 60 GB 必要。 最大ストレージ容量は 750 GB 以下。 **注:** インストール プロセスの中で、使用可能なディスク領域に ACS がパーティションを自動的に作成します。 **注:** ログ コレクタとして機能するセカンダリ インスタンスには、500 GB よりも大きいハード ディスク サイズを割り当てることを推奨します。
NIC（ネットワーク インターフェイス カード）	1 GB の専用 NIC インターフェイス
ハイパーバイザ	■ VMware ESXi 5.5 ■ VMware ESXi 5.5 Update 1 ■ VMware ESXi 5.5 Update 2 ■ VMware ESXi 6.0

注:仮想マシンにインストールされた ACS を ACS 5.8.1 にアップグレードする場合は、仮想マシンのディスク容量が 500 GB 以上であることが必要です。

ACS 5.8.1 のディスク領域管理メカニズムがシステムを自動的に管理し、ファイル システム上に使用可能なファイル ボリュームを、ローカル ストア、コンフィギュレーション、キャッシュなどファイル タイプ別に設定します。実際のファイル サイズ制限は、ハード コードされた相対ディスク クォータ設定(パーセンテージ)に基づいて、ディスク サイズを入力として使用し、インストール時に計算されます。ただし、ACS データベース ログのサイズは固定されています。ACS 5.8.1 は、VMware インスタンスの作成時に選択したディスク サイズに基づいて、60 GB ～ 750 GB の間の使用可能なハード ディスク サイズにインストールされます。インストール後に ACS ディスクのサイズを変更するには、次の手順を実行します。

- データをバックアップする。
- ACS アプリケーションのイメージを再作成するか、アプリケーションを新規インストールします。
- バックアップしたデータを復元します。

バックアップしたデータの復元中、バックアップ サイズまたは ACS View のデータベース サイズが対応するディスク クォータを超過した場合は、警告メッセージが表示されます。ただし、復元動作は中断されません。復元動作が失敗するのは、/opt パーティション サイズのハード制限に達した場合だけです。

ACS 5.8.1 では、ログ コレクタ サーバを 60 GB のディスク領域にインストールできます。通常、ACS View のログ コレクタ ノードには、ログとレポートのデータベースのメンテナンス用にさらに容量が必要です。そのため、ログ コレクタ サーバとして機能するセカンダリ インスタンスの推奨ディスク サイズは 500 GB です。

ログ コレクタ サーバに 60 GB を割り当てた場合、View データベースは 5.8.1 GB だけになります。その結果、一部の機能が正常に動作しなくなることがあります。このような影響を受ける機能には、バックアップ、フル バックアップ、差分バックアップ、リカバリのロギング、パージ、データベース圧縮動作などがあります。

VMware インスタンスの作成時には、その VMware インスタンスに割り当てるリソースが、CPU コア数、RAM、およびディスクに関して、VMware ホスト サーバの実際の物理リソースを超えていないことを確認してください。たとえば、VMware ホスト サーバの合計 CPU コア数が 10 の場合、そのホスト サーバ上に作成される VMware インスタンスに割り当てられた CPU コア数の合計が、10 を超えてはいけません。

注:VM にホストされる大規模な ACS の分散導入環境では、すべての VM ホスティング サーバの CPU を同じベンダーのものにすることを推奨します。

注:いずれかの VMware ホストでハイパー スレッディングを有効にする場合は、同じ導入の中で ACS VM をホストするすべての VMware ホストでも必ず有効にすることを推奨します。

注:ACS 5.8.1 を(1 つの論理ボリューム マネージャ(LVM)ディスクを定義して)複数のディスクにインストールすることはできません。

VMWare サーバのインストール

デフォルトのオプションと適切な IP アドレスで VMware サーバをインストールします。

VMware vSphere Client のインストール

リモートの場所から VMware サーバにアクセスするには、VMware vSphere クライアントを使用します。

VMware vSphere Client をインストールするには、次の手順を実行します。

1. 次のリンクに移動します。

   http://*IP address of VMware server*

   このリンクにアクセスするには、有効な Cisco.com ログイン クレデンシャルが必要です。

2. [Download] をクリックして、VMware vSphere クライアント ソフトウェアをダウンロードします。
3. インストーラを実行します。

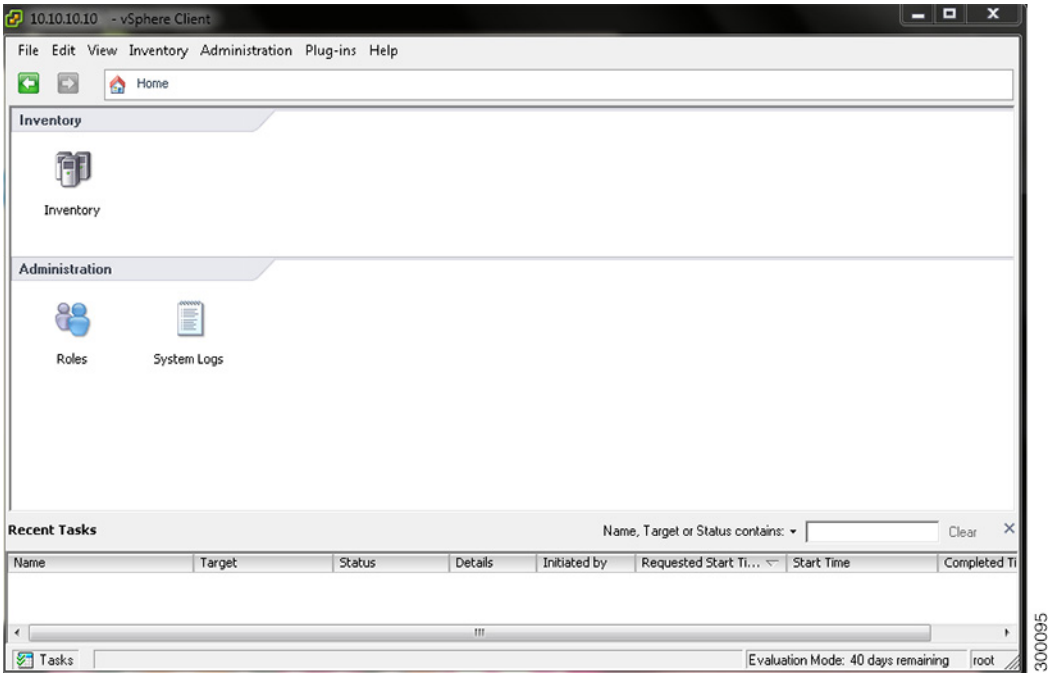
4. VMware サーバにログインします。

   図 1(3 ページ) に、VMware サーバのログイン ウィンドウを示します。

図 1　　ログイン ウィンドウ

vSphere クライアント ウィンドウが表示されます。(図 2(3 ページ))。

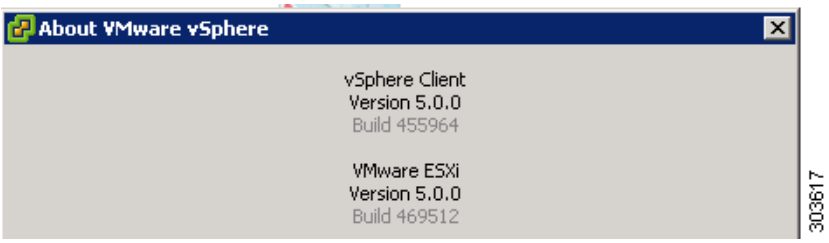
図 2　　vSphere クライアント ウィンドウ



5. [Help] > [About VMware vSphere] を選択して、VMware ESX と vSphere クライアントのバージョンを確認します。

   図 3(4 ページ) に、VMware vSphere のバージョンを示します。

図 3　About VMware vSphere



ESXi 5.5 および ESXi 6.0 用 VM の設定

ホストは ESX サーバなどの仮想化ソフトウェアを使用して仮想マシンを実行します。ホストは、ストレージにアクセスし、ネットワークに接続するために CPU およびメモリ リソースを仮想マシンに提供します。

ここでは、VMware vSphere Client を使用した VM 設定プロセスについて説明します。

ESXi 5.5 および ESXi 6.0 用 VM を設定するには、次の手順を実行します。

1. ESX サーバにログインします。
2. [Inventory] をクリックします。
3. VMware vSphere Client の左ペインのホスト コンテナを右クリックし、[New Virtual Machine] 選択します。

   [Create New Virtual Machine] ウィザードが表示されます。
4. [Configuration Type] ダイアログボックスで、図 4(4 ページ) に示すように VM 設定として [Typical] を選択して、[Next] をクリックします。

図 4　[Virtual Machine Configuration] ダイアログボックス

   [Name and Location] ダイアログボックスが表示されます。(図 5(4 ページ))。
5. VM を参照するために使用する名前を入力して、[Next] をクリックします。

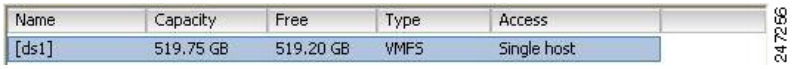
図 5　[Name and Location] ダイアログボックス

注:VM ホストに使用するホスト名を使用します。

[Data Storage] ダイアログボックスが表示されます。(図 6(5 ページ))。

6. 最低 500 GB の空きスペースが使用可能なデータ ストアを選択し、[Next] をクリックします。

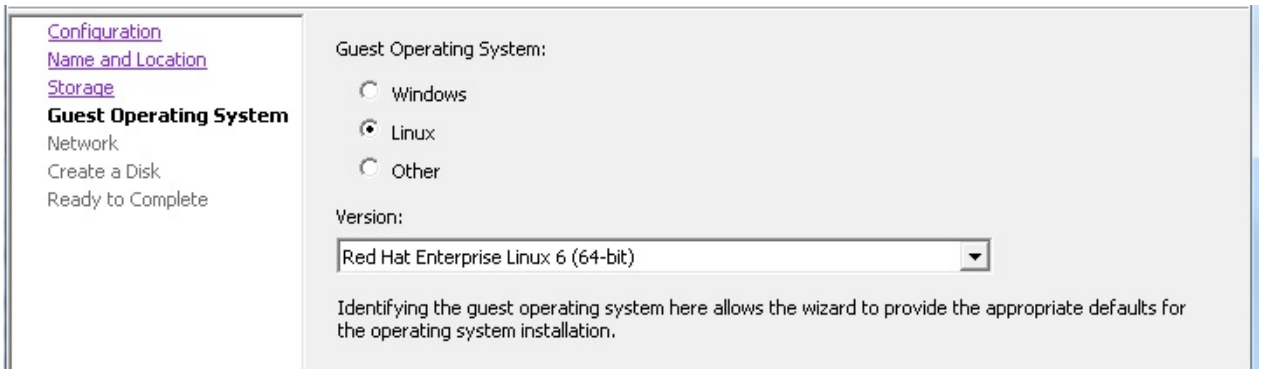
図 6　[Data Storage] ダイアログボックス



[Guest Operating System] ダイアログボックスが表示されます。(図 7(5 ページ))。

7. [Linux] オプション ボタンをクリックし、[Version] ドロップダウンリストから [Red Hat Enterprise Linux 6 (64-bit)] を選択し、[Next] をクリックします。

図 7　[Guest Operating System] ダイアログボックス

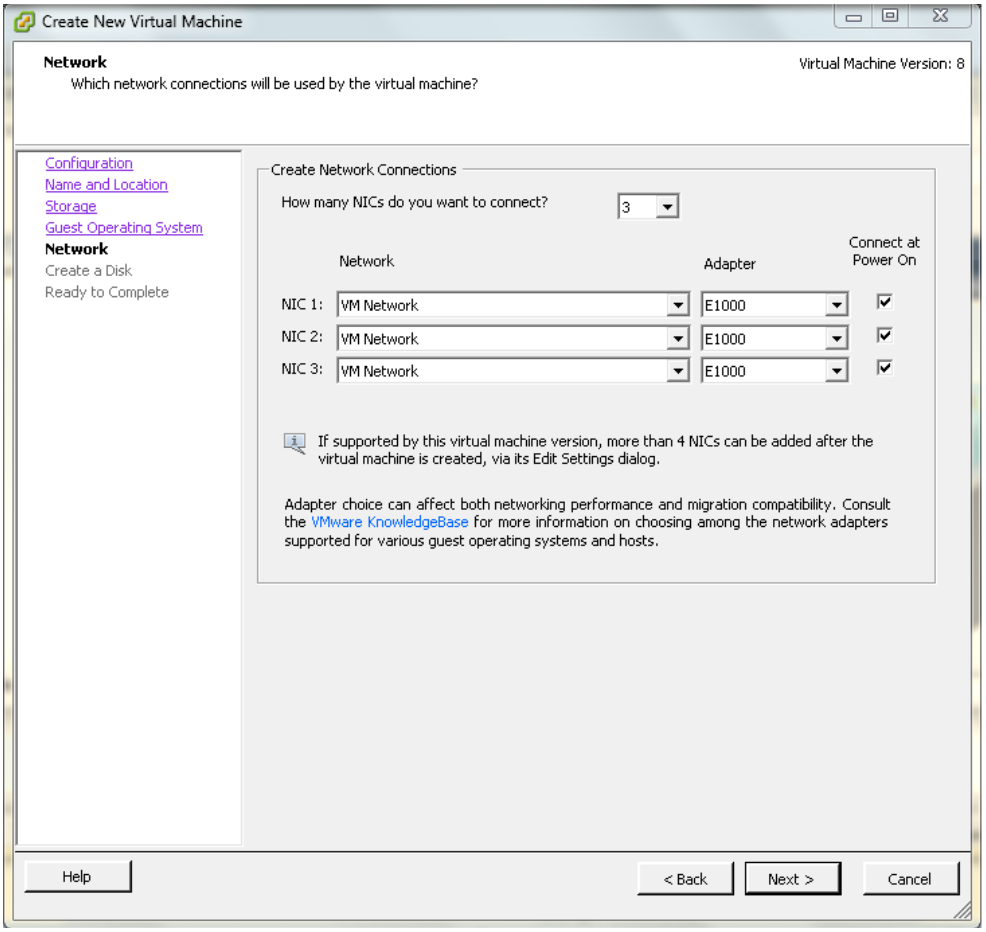


[Network] ダイアログボックスが表示されます。(図 8(6 ページ))。

8. [Network] ウィンドウで使用する NIC の数を選択し、[Next] をクリックします。使用できる NIC は 4 つまでです。

注:ACS は、VMXNET2(拡張)および VMXNET3 アダプタをサポートしていません。

図 8　[Network] ダイアログボックス

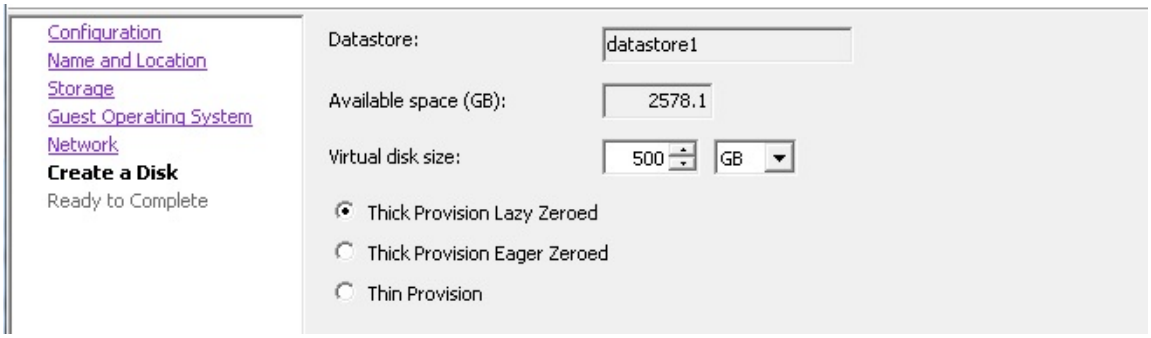


[Create a Disk] ダイアログボックスが表示されます。(図 9(6 ページ))。

9. [Virtual Disk Capacity] ウィンドウで 500 GB のディスク サイズを選択し、[Next] をクリックします。

注:最小仮想ディスク領域要件は 60 GB に設定できます。仮想ディスク領域として 60 GB を使用すると、重大な問題が発生することがあります。回避策については、「トラブルシューティング」の項で説明します。

図 9　[Create a Disk] ダイアログボックス



[Ready to Complete] ダイアログボックスが表示されます。図 10（7 ページ）

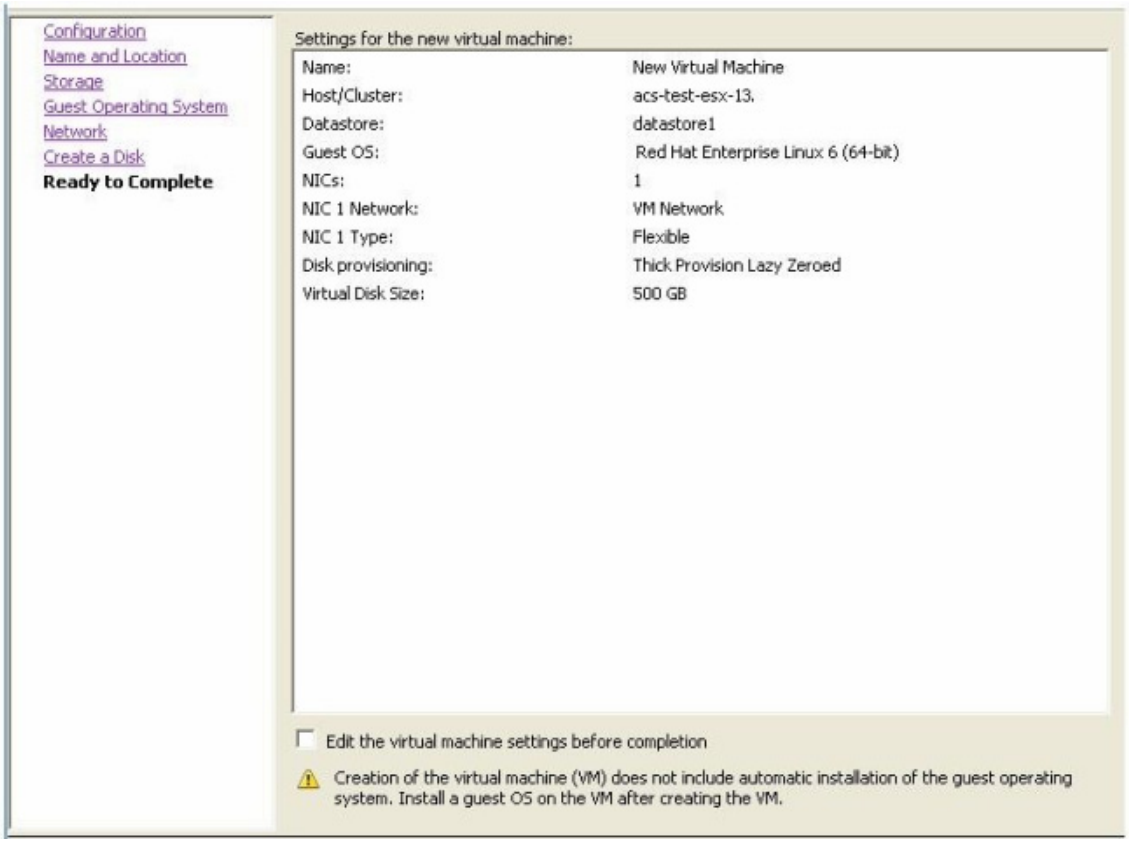
注:ACS はサポートしているすべての VMWare においてシン プロビジョニングのみをサポートしているため、ストレージ タイプに VMWare シン プロビジョニングを選択しないでください。

ACS がシン プロビジョニング ストレージ タイプの VMware にインストールされている場合は、次のことが推奨されます。

1. ACS 構成をバックアップします。
2. シック プロビジョニング ストレージ タイプで VMware を再イメージ化します。
3. 新たに変換されたシック プロビジョニングされているストレージ VMware にバックアップを復元します。

   注:RAM、CPU、ディスクなどのハードウェア リソースを仮想マシンにプロビジョニングし過ぎないでください。
4. 新規作成された VM の [Name]、[Guest OS]、[Virtual CPU]、[Memory]、および [Virtual Disk Size] など、設定の詳細を確認します。

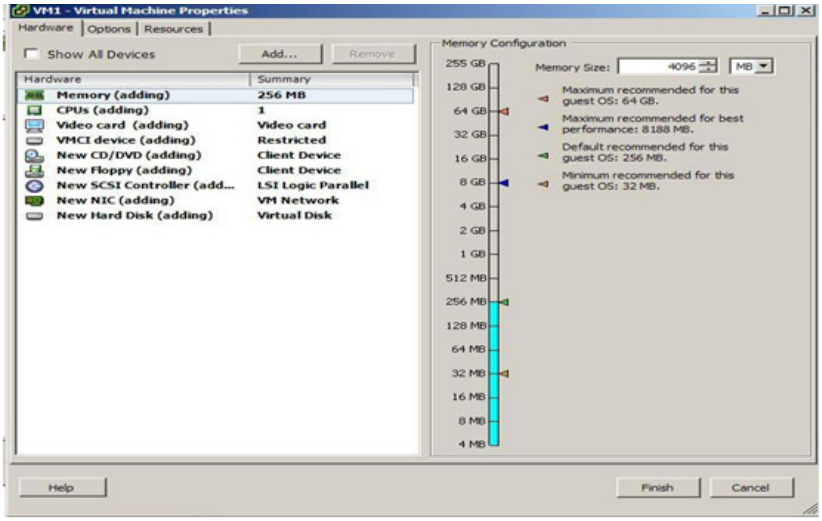
図 10　[Ready to Complete] ダイアログボックス



5. [Edit the virtual machine settings before completion] チェックボックスをオンにし、[Next] をクリックします。

   [Memory Configuration] ダイアログボックスが表示されます。（図 11（8 ページ））。
6. **4096 MB** と入力して、[Next] をクリックします。

図 11　[Memory Configuration] ダイアログボックス



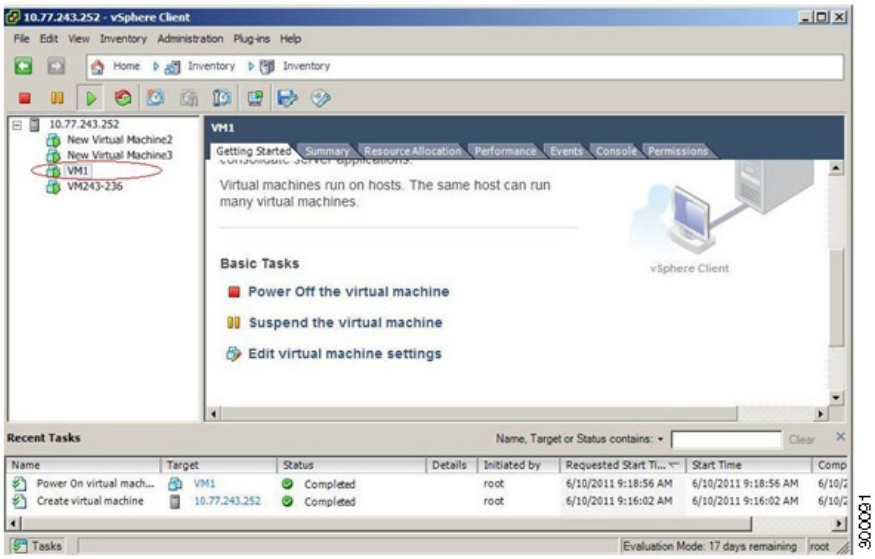
[Number of Virtual Processors] ダイアログボックスが表示されます。(図 12(8 ページ))。

7. [Number of virtual processors] ドロップダウン リストから、[2](2 つ使用可能な場合)を選択します。または、任意の数を選択して [Finish] をクリックすることもできます。

図 12　[Number of Virtual Processors] ダイアログボックス

8. 仮想マシンがインストールされ、次のように VMware ドロワーにリストされます。

図 13　vSphere Client



ACS サーバをインストールするための VM の準備

VM を設定したら、ACS リリース 5.8.1 をインストールできます。ACS インストール ディスクから ACS サーバをインストールするには、ACS インストール ディスクから起動するよう VM を設定する必要があります。

ACS 5.8.1 DVD からブートするよう、VM で仮想 DVD ドライブを設定する必要があります。

これは、ご使用の環境に応じて異なる方法を使用して実行できます。

VMware ESX サーバ ホストの DVD ドライブを使用して VM を設定するには、DVD ドライブを使用した VM の設定（9 ページ）を参照してください。

DVD ドライブを使用した VM の設定

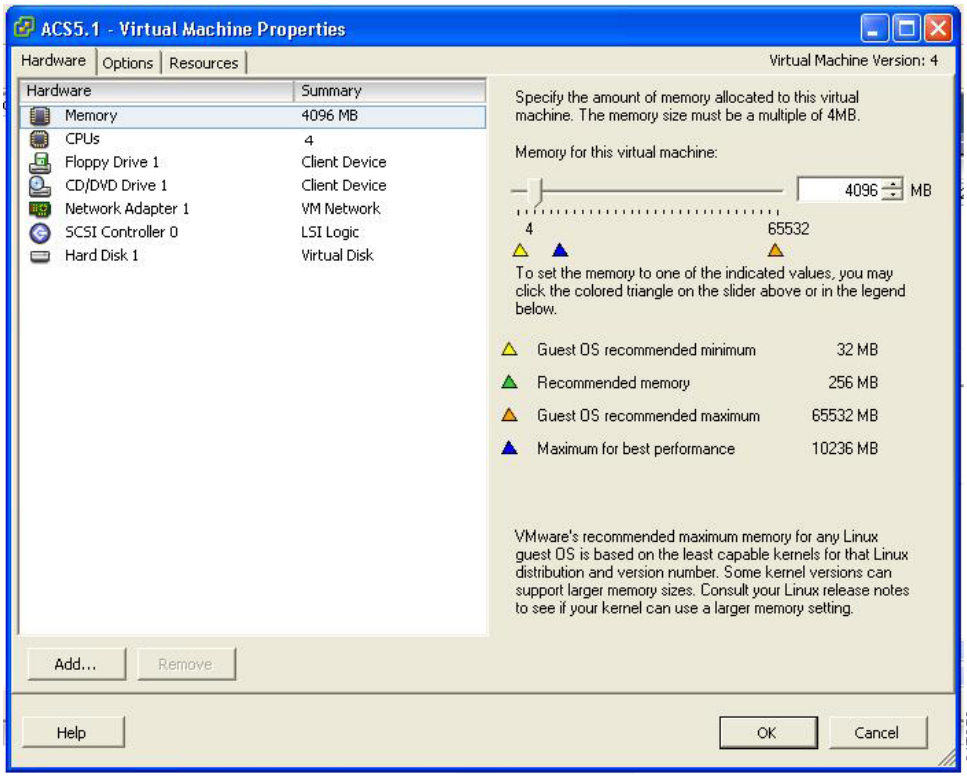
ここでは、VMware ESX サーバ ホストの DVD ドライブを使用して ACS インストール ディスクから起動するよう VM を設定する方法について説明します。

DVD ドライブを使用して VM を設定するには、次の手順を実行します。

1. VMware vSphere Client で、新たに作成した VM を強調表示して、[Edit Virtual Machine Settings] を選択します。

   [Virtual Machine Properties] ウィンドウが表示されます。図 14（9 ページ）に、名前 ACS.5.8.1 で作成される VM のプロパティを示します。

図 14　[Virtual Machine Properties] ダイアログボックス



2. [Virtual Machine Properties] ダイアログボックスで、[CD/DVD Drive 1] を選択します。

   [CD/DVD Drive1 properties] ダイアログボックスが表示されます。

3. [Host Device] オプションを選択して、ドロップダウン リストからご使用の DVD ホスト デバイスを選択します。
4. [Connect at Power On] オプションを選択して、[OK] をクリックして設定を保存します。

   これで、VMware ESX サーバの DVD ドライブを使用して、ACS サーバをインストールできるようになりました。

設定が完了したら、[Console] タブをクリックして、左側のペインから VM を右クリックし、[GUEST] > [Send Ctrl+Alt+Del] を選択して VM を再起動します。

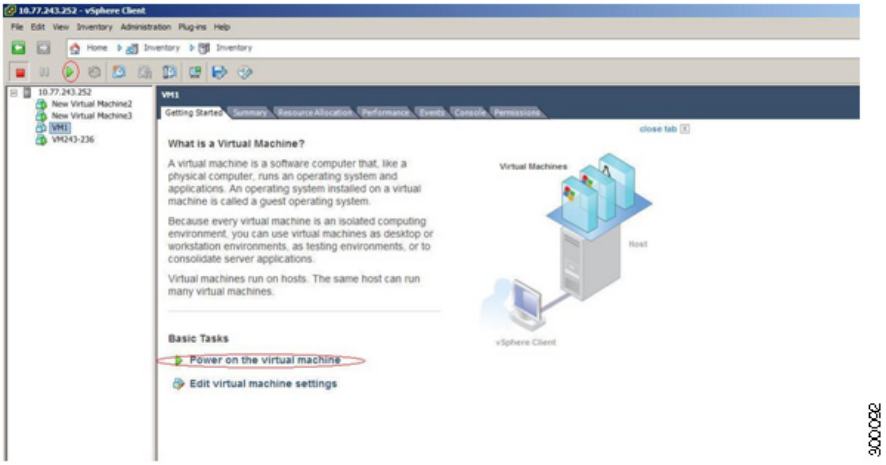
ESXi 5.5 および 6.0 での ACS サーバのインストール

ここでは、VMware ESXi 5.5 および ESXi 6.0 での ACS 5.8.1 のインストール方法について説明します。

ACS 5.8.1 サーバをインストールするには、次の手順を実行します。

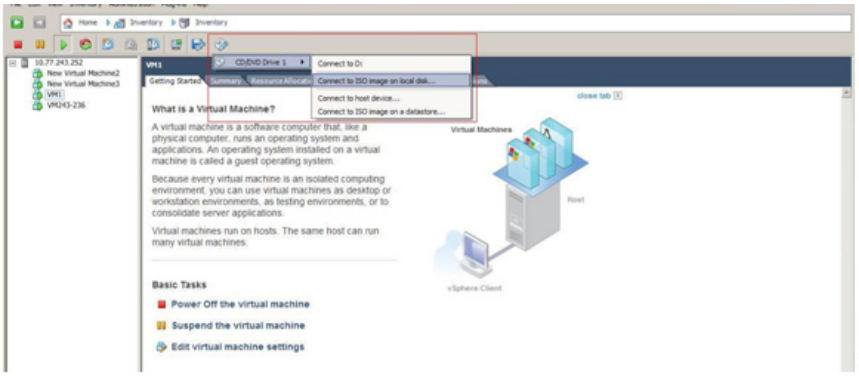
1. VMware vSphere Client にログインします。
2. ACS 5.8.1 インストール ディスクを VMware ESX ホストの CD/DVD ドライブに挿入し、VM の電源をオンにします。

図 15　　仮想マシンの電源をオンにします。



3. VMware Server にアクセスするために、ACS 5.8.1 リカバリ ISO イメージを VMware vSphere クライアントに保存します。
4. ツールバーの CD アイコンをクリックし、[Connect CD/DVD 1] > [Connect to ISO image on local disk] を選択します。

図 16　　ローカル ディスク上の ISO イメージへの接続



5. ブラウズして ACS 5.8.1 ISO イメージを探します。

   [console] タブに移動します。[console] タブに移動すると、すぐにカーソルの制御が失われます。

6. **Ctrl+Alt** を押し、カーソルの制御を取得します。

7. **Enter** キーを押します。

   ACS 5.8.1 リカバリ ISO イメージがロードされた状態で、マシンが再起動されます。この時点で、ユーザに ACS 5.8.1 のインストール オプションが提示されます。

   ACS 5.8.1 インストール ディスクが起動したら、コンソールに次の内容が表示されます。

```
Welcome to Cisco Secure ACS 5.8.1 Recovery
To boot from the hard disk press <Enter>
Available boot options:
[1] Cisco Secure ACS 5.8.1 Installation (Monitor/Keyboard)
[2] Cisco Secure ACS 5.8.1 Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot: 1
```

   初期セットアップを実行するには、モニタとキーボード ポートまたはコンソール ポートのいずれかを選択できます。

8. システム プロンプトで、**1** と入力してモニタとキーボード ポートを選択するか、**2** と入力してコンソール ポートを選択し、**Enter** を押します。

   VM で ACS のインストールが開始します。

   注: インストール プロセスが完了するまで、20 分かかります。

   インストール プロセスが終了すると、VM は自動的に再起動します。

   VM の再起動時に、コンソールに次のように表示されます。

```
Type 'setup' to configure your appliance
localhost:
```

9. システム プロンプトで、**setup** と入力し、**Enter** を押します。

   セットアップ ウィザードが表示され、ウィザードに従って初期設定を実行します。

   コンソールで、次のパラメータを入力するよう求められます。

```
localhost login: setup
Enter hostname[]: acs54-server-1
Enter IP address[]: a.b.c.d
Enter IP default netmask[]: 255.255.255.255
Enter IP default gateway[]: a.b.c.d
Enter default DNS domain[]: mycompany.com
Enter primary nameserver[]: a.b.c.d
Add secondary nameserver? Y/N : n
Add primary NTP server [time.nist.gov]: a.b.c.d
Add secondary NTP server? Y/N : n
Enter system timezone[UTC]:
Enable SSH service? Y/N [N] : y
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Virtual machine detected, configuring VMware tools...
File descriptor 4 (/opt/system/etc/debugd-fifo) leaked on lvm.static invocation
Parent PID 3036: /bin/bash
Do not use `Ctrl-C' from this point on...
debugd[2455]: [2809]: config:network: main.c[252] [setup]: Setup is complete.
Installing applications...
Installing acs...
Generating configuration...
Rebooting...
```

セットアップ プロセスの詳細については、セットアップ プログラムの実行（2 ページ）を参照してください。

VMWare 強化の要件

VMware 仮想マシンが実行されている VMware サーバとオペレーティング システムの両方を、VMware とオペレーティング システムのベンダーによって指定されたガイドラインに従って強化する必要があります。

詳細については、VMware サポート Web サイトを参照してください。次のリンクが役立ちます。

- http://www.vmware.com/support/
- http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1017910
- http://communities.vmware.com/community/vmtn

VMware ツールのサポート

ACS 5.8.1 は VMware ツール 9.0.0 をサポートしています。ACS 5.8.1 で VMware ツールを使用すると、次のような利点があります。

- NIC パフォーマンスの向上
- Small Computer System Interface（SCSI）の I/O パフォーマンスの向上
- ゲスト オペレーティング システムとホストの時刻同期

セットアップ ウィザードを初めて実行したときに、「`Virtual machine detected, configuring VMware Tools`」という新しいテキスト行が表示されます。VMware ツールがインストールされているかどうか確認するには、次の方法もあります。

vSphere クライアントで仮想マシンの [Summary] タブをクリックします。VMware ツールに対して「Running」のテキストが表示されます。これで、VMware ツールがインストールされ、実行されていることを確認できます。

CLI コマンドの **show inventory** を使用できます。この CLI を実行すると、NIC ドライバ情報を示すリストが表示されます。VMware ツールがインストールされている場合は、リストにドライバ情報が [VMware Virtual Ethernet Driver] と表示されます。

リリース 5.8.1 への ACS のアップグレード

Cisco Secure Access Control システムのアップグレード

この章では ACS 導入またはスタンドアロン ACS サーバを（5.5、5.6、5.7、5.8 の最新のパッチ適用後に）5.5、5.6、5.7 から 5.8.1 にアップグレードする方法について説明します。

注：ACS 5.0、5.1、5.2、5.3、5.4 を使用している場合は、まず ACS 5.5、5.6、5.7、5.8 にアップグレードしてから ACS 5.8.1 にアップグレードする必要があります。

この章のシナリオは次のとおりです。

- ACS 導入の 5.8 から 5.8.1 へのアップグレード（2 ページ）
- ACS 導入の 5.7 から 5.8.1 へのアップグレード（10 ページ）
- ACS 導入の 5.6 から 5.8.1 へのアップグレード（10 ページ）
- ACS 導入の 5.5 から 5.8.1 へのアップグレード（10 ページ）
- ACS サーバの 5.8 から 5.8.1 へのアップグレード（10 ページ）

  次の手順のいずれかを使用できます。

  - アプリケーション アップグレード バンドルを使用した ACS サーバのアップグレード（10 ページ）：ACS サーバの 5.6 から 5.8.1 への差分アップグレードを行う手順。
  - ACS サーバの再イメージ化とアップグレード（11 ページ）：ACS 5.6 アプリケーション データをバックアップし、ACS 5.8.1 で復元する手順。
- ACS サーバの 5.7 から 5.8.1 へのアップグレード（13 ページ）
- ACS サーバの 5.6 から 5.8.1 へのアップグレード（13 ページ）
- ACS サーバの 5.5 から 5.8.1 へのアップグレード（13 ページ）
- ACS パッチの適用（13 ページ）
- CSACS-1121 上の ACS 5.5、5.6、5.7、5.8 の ACS 5.8.1 使用 Cisco SNS 3400 シリーズ アプライアンスへのアップグレード（14 ページ）
- CSACS-1121 または SNS-3400 上の ACS 5.5、5.6、5.7、5.8 の ACS 5.8.1 使用 Cisco SNS 3500 シリーズ アプライアンスへのアップグレード（15 ページ）

アップグレード プロセスでは ACS サーバのアップグレードが必要です。これには、Monitoring and Report Viewer およびデータベース内の設定情報が含まれます。

注：ACS 5.8.1 は、アプリケーションのアップグレードの一部として ADE-OS 1.x を 2.x にアップグレードします。

ACS はアップグレード プロセス中に ACS サーバを 5.8.1 にアップグレードし、データを ACS 5.8.1 サーバに復元します。復元操作の一部として、ACS は設定データを 5.8.1 互換形式に変換します。

ACS はデータ アップグレード情報を acsupgrade.log ファイルに格納します。このログ ファイルの内容を表示するには、サポート バンドルをダウンロードします。

サポート バンドルのダウンロードの詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。また、ACS CLI で実行されたすべての操作の詳細が記録されている ADE.log も参照してください。ACS を 4.*x* から 5.8.1 に移行する場合は、『*Migration Guide for Cisco Secure Access Control System 5.8.1*』で説明している移行手順に従ってください。

ACS アップグレードを実行するには、(TFTP リポジトリではなく)FTP、ネットワーク ファイル システム(NFS)、またはセキュア FTP(SFTP)ネットワーク サーバが設定されたリポジトリが必要です。

リポジトリを作成するには、**repository** コマンドを使用します。この章で使用しているコマンドの詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。

アップグレード パス

ACS サーバを 5.x バージョンから ACS 5.8.1 にアップグレードする際には、次のアップグレード パスを使用できます。

- **パス 1**:ACS 5.8 から ACS 5.8.1 へ。ACS 5.8 から 5.8.1 へアップグレードするには、ACS サーバの 5.8 から 5.8.1 へのアップグレード(10 ページ)を参照してください。
- **パス 2**:ACS 5.7 から ACS 5.8.1 へ。ACS 5.7 から 5.8.1 へアップグレードするには、ACS サーバの 5.8 から 5.8.1 へのアップグレード(10 ページ)を参照してください。
- **パス 3**:ACS 5.6 から ACS 5.8.1 へ。ACS 5.6 から 5.8.1 へアップグレードするには、ACS サーバの 5.7 から 5.8.1 へのアップグレード(13 ページ)を参照してください。
- **パス 4**:ACS 5.5 から ACS 5.8.1 へ。ACS 5.5 から 5.8.1 へアップグレードするには、ACS サーバの 5.6 から 5.8.1 へのアップグレード(13 ページ)を参照してください。
- **パス 5**:ACS 5.4 から ACS 5.6、次に ACS 5.8.1 へ。ACS 5.4 から ACS 5.6 へアップグレードするには、『*Installation and Upgrade Guide for Cisco Secure Access Control System 5.6*』を参照してください。ACS 5.6 から 5.8.1 へアップグレードするには、ACS サーバの 5.7 から 5.8.1 へのアップグレード(13 ページ)を参照してください。
- **パス 6**: ACS 5.3 から ACS 5.5、次に ACS 5.8.1 へ。ACS 5.3 から ACS 5.5 へアップグレードするには、『*Installation and Upgrade Guide for Cisco Secure Access Control System 5.5*』を参照してください。ACS 5.5 から 5.8.1 へアップグレードするには、ACS サーバの 5.6 から 5.8.1 へのアップグレード(13 ページ)を参照してください。
- **パス 7**:ACS 5.2 から ACS 5.4、次に ACS 5.6、そして ACS 5.8.1 へ。ACS 5.2 から ACS 5.4 へアップグレードするには、『*Installation and Upgrade Guide for Cisco Secure Access Control System 5.4*』を参照してください。ACS 5.4 から 5.8.1 へアップグレードするには、パス 4 を使用します。
- **パス 8**:ACS 5.1 から ACS 5.3、次に ACS 5.5、そして ACS 5.8.1 へ。ACS 5.1 から ACS 5.3 へアップグレードするには、『*Installation and Upgrade Guide for Cisco Secure Access Control System 5.3*』を参照してください。ACS 5.3 から 5.8.1 へアップグレードするには、パス 5 を使用します。
- **パス 9**:ACS 5.0 から ACS 5.2、次に ACS 5.4、そして ACS 5.6、ACS 5.8.1 へ。ACS 5.0 から ACS 5.2 へアップグレードするには、『*Installation and Upgrade Guide for Cisco Secure Access Control System 5.2*』を参照してください。ACS 5.2 から 5.8.1 へアップグレードするには、パス 6 を使用します。

注:仮想マシンにインストールされた ACS を ACS 5.8.1 にアップグレードする場合は、仮想マシンのディスク容量が 500 GB 以上であることが必要です。

ACS 導入の 5.8 から 5.8.1 へのアップグレード

ACS 5.8 導入を ACS 5.8.1 にアップグレードするには、この項で説明されている手順に従ってください。導入のアップグレード プロセスは、次の各段階で構成されます。

- ログ コレクタ サーバのアップグレード(3 ページ)
- セカンダリ サーバのアップグレード(6 ページ)
- プライマリ サーバのアップグレード(8 ページ)

注:ACS 5.8 導入と ACS 5.8.1 導入との相互運用性はサポートされていません。

複数の ACS インスタンスが関わる導入シナリオでは通常、プライマリ ACS インスタンスが設定データのマスター データベースとして機能し、セカンダリ ACS インスタンスの 1 つが監視およびレポート データを格納します。プライマリ インスタンスを使用して監視およびレポート データを保存することも可能です。

最初に、ログ コレクタ サーバを ACS 5.8.1 にアップグレードし、すべてのサーバの 5.8.1 へのアップグレードが完了するまで、このサーバを ACS 5.8 導入と 5.8.1 導入間の共通のログ コレクタとして使用します。

この通常のセットアップにはいくつかの例外があります。これは、次に説明されているように対処できます。

ご使用の 5.8.1 導入で、ACS 5.8 のプライマリ サーバがログ コレクタとして機能している場合は、既存のプライマリ サーバをアップグレードする前に、導入のセカンダリ サーバのいずれかをプライマリに昇格させる必要があります。セカンダリ サーバのプライマリへのプロモート（9 ページ）を参照してください。

注: セカンダリ サーバをアップグレードする際には、先にプライマリ サーバからそのサーバを登録解除しておく必要があります。

ログ コレクタ サーバのアップグレード

ログ コレクタ サーバを ACS 5.8.1 にアップグレードするには、次の手順を実行します。

1. ログ コレクタにするセカンダリ サーバを選択します。

   a. プライマリ ACS サーバから、[System Administration] > [Configuration] > [Log Configuration] > [Log Collector] を選択します。

   [Log Collector] ページが表示されます。

   b. [Select Log Collector Server] ドロップ ダウン リストから、ログ コレクタにする新しいセカンダリ インスタンスを選択し、[Set Log Collector] をクリックします。

   新しいセカンダリ ログ コレクタの ACS サービスが再起動されます。

2. EXEC モードで **show application status acs** コマンドを入力して、すべてのプロセスが正常に稼働しているかどうかを確認し、Enter を押します。

   コンソールに次のメッセージが表示されます。

```
Process 'database'                running
Process 'management'              running
Process 'runtime'                 running
Process 'adclient'                running
Process 'ntpd'                    running
Process 'view-database'           running
Process 'view-jobmanager'         running
Process 'view-alertmanager'       running
Process 'view-collector'          running
Process 'view-logprocessor'       running
```

   これで、すべてのプロセスが稼働していることを確認できました。

3. 古いログ コレクタ サーバを導入から登録解除し、ACS 5.8 プライマリ サーバから削除して、サーバがスタンドアロン サーバになるようにします。

   a. ACS 5.8 プライマリ サーバの Web インターフェイスから、[System Administration] > [Operations] > [Distributed System Management] を選択します。

   [Distributed System Management] ページが表示されます。

   b. [Secondary Instances] テーブルから、登録解除するセカンダリ インスタンスの横にあるチェックボックスをオンにします。

   c. [Deregister] をクリックします。

システムに次のメッセージが表示されます。

```
This operation will deregister the selected ACS Instance from the Primary Instance.

Do you wish to continue?
```

d. [OK] をクリックします。

セカンダリ インスタンス(古いログ コレクタ)サービスが再起動されます。

e. ACS 5.8 プライマリ サーバにログインします。

f. [System Administration] > [Operations] > [Distributed System Management] を選択します。

g. [Secondary Instances] テーブルから、削除する登録解除済みのセカンダリ インスタンスの横にあるチェックボックスをオンにします。

h. [Delete] をクリックします。

次のメッセージが表示されます。

```
Are you sure you want to delete the selected item/items?
```

i. [OK] をクリックします。

[Distributed System Management] ページの [Secondary Instances] テーブルが表示されます。このとき、削除されたセカンダリ インスタンスは表示されません。

4. ログ コレクタ データをバックアップします。

ACS CLI から、EXEC モードで次の **backup** コマンドを入力して、バックアップを実行し、バックアップをリモート リポジトリに格納します。

backup *backup-file-name* **repository** *repository-name*

注:データをバックアップする際、データのサイズが ACS に割り当てられているディスク クォータを超える場合、CLI に警告メッセージが表示され、ACS Monitoring and Reports のアラームが起動します。

5. 古い ACS ログ コレクタをアップグレードします。

ACS サーバの 5.8 から 5.8.1 へのアップグレード(10 ページ)の手順を実行します。

ログ コレクタ サーバですべてのプロセスが稼働状態になったら、Monitoring and Report Viewer を確認します。それには、[Monitoring Configuration] > [System Operations] > [Data Upgrade Status] を選択し、アップグレードが成功したかを確認します。Monitoring and Report Viewer データ アップグレードのステータスを示す [Data Upgrade Status] ページが表示されます。

データベース アップグレードが完了すると、ACS に次のメッセージが表示されます。

アップグレードが正常に完了しました。

これで、古いログ コレクタが 5.8.1 にアップグレードされ、ACS 5.8.1 スタンドアロン プライマリ サーバまたはログ コレクタとして動作するようになりました。詳細については、ACS Monitoring and Report Viewer のアップグレード(9 ページ)を参照してください。

6. 5.8.1 ログ コレクタを 5.8 導入のリモート ログ ターゲットとして定義します。

a. [System Administration] > [Configuration] > [Log Configuration] > [Remote Log Targets] を選択します。

[Remote Log Targets] ページが表示されます。

b. [Create] をクリックします。

[Create] ページが表示されます。

c. 次のフィールドに値を入力します。

- [Name]：リモート ログ ターゲットの名前。最大長は 32 文字です。
- [Description]：（任意）リモート ログ ターゲットの説明。説明の最大長は 1024 文字です。
- [Type]：リモート ログ ターゲットのタイプ。[Syslog] が唯一のオプションです。
- [IP Address]：*x.x.x.x* 形式のリモート ログ ターゲットの IP アドレス。5.8.1 ログ コレクタ サーバの IP アドレスを指定します。
- [Use Advanced Syslog Options]：ポート番号、ファシリティ コード、および最大長を含む詳細 Syslog オプションを有効にする場合にクリックします。
- [Port]：ACS とリモート ログ ターゲット間の通信チャネルとして使用するリモート ログ ターゲットのポート番号（デフォルトは 514）。ポート番号には **20514** を入力します。
- [Facility Code]：（任意）[Facility Code] ドロップダウン リストからオプションを選択します。
- [Maximum Length]：リモート ログ ターゲット メッセージの最大長。有効なオプションは 200 ～ 8192 です。

d. [Submit] をクリックします。

リモート ログ ターゲット設定が保存されます。新しいリモート ログ ターゲット設定が示された [Remote Log Targets] ページが表示されます。

これで、5.8 導入からの認証の詳細が 5.8 ログ コレクタ サーバと 5.8.1 ログ コレクタ サーバの両方に記録されるようになりました。

7. 5.8 プライマリ サーバでは、リモート ログ ターゲットに適したロギング カテゴリを設定します。

a. [System Administration] > [Configuration] > [Log Configuration] > [Logging Categories] > [Global] を選択します。

[Logging Categories] ページが表示されます。このページから、ロギング カテゴリを参照できます。

b. 設定するロギング カテゴリの名前をクリックするか、設定するロギング カテゴリの名前の横にあるオプション ボタンをクリックして [Edit] をクリックします。

c. [General] タブで、次のフィールドに入力します。

- [Log Severity]：ドロップダウン リストを使用して、重大度レベルを選択します。有効なオプションは [FATAL]、[ERROR]、[WARN]、[INFO]、および [DEBUG] です。
- [Log to Local Target]：ローカル ターゲットへのロギングをイネーブルにする場合にオンにします。
- [Local Target is Critical]：このローカル ターゲットをクリティカル ターゲットにする場合にチェックボックスをオンにします。アカウンティングおよび AAA 監査（Passed Authentication）ロギング カテゴリ タイプの場合にのみ使用できます。

d. [Remote Syslog Target] タブをクリックして、[Remote Targets] を選択してログを表示します。

e. [Submit] をクリックします。

設定したロギング カテゴリが示された [Logging Categories] ページが表示されます。セカンダリ サーバのアップグレード（6 ページ）に進みます。

セカンダリ サーバのアップグレード

導入内の各 ACS 5.8 セカンダリ サーバを ACS 5.8.1 にアップグレードするには、この手順を使用します。

注: セカンダリ サーバのローカルの証明書を保持するには、各セカンダリ サーバをプライマリ ロールに昇格させてから、ACS 5.8.1 へのアップグレードを行う必要があります。

セカンダリ ACS サーバをアップグレードする前に、サーバがアクティブであること、およびローカル モードになっていないことを確認します。

セカンダリ サーバの Web インターフェイスからステータスを確認するには、[System Administration] > [Operations] > [Local Operations] を選択します。

1. セカンダリ サーバがログ コレクタであるかどうかを確認します。ログ コレクタである場合は、ログ コレクタ サーバを他の任意のセカンダリ サーバに変更します。ログ コレクタではない場合は、ステップ 2 に進みます。

   a. ACS 5.8 プライマリ サーバで、[System Administration] > [Configuration] > [Log Configuration] > [Log Collector] を選択します。

   ACS に、現在のログ コレクタ サーバが表示されます。

   b. [Select Log Collector] ドロップダウンリストから、ログ コレクタに設定する別のサーバを選択します。

   c. [Set Log Collector] をクリックします。

2. セカンダリ サーバを 5.8 導入から登録解除し、ACS 5.8 プライマリ サーバから削除して、サーバがスタンドアロン サーバになるようにします。

   a. [System Administration] > [Operations] > [Distributed System Management] を選択します。

   [Distributed System Management] ページが表示されます。

   b. [Secondary Instances] テーブルから、登録解除するセカンダリ インスタンスの横にあるチェックボックスをオンにします。

   c. [登録解除(Deregister)] をクリックします。

   システムに次のメッセージが表示されます。

   ```
   This operation will deregister the selected ACS Instance from the Primary Instance.

   Do you wish to continue?
   ```

   d. [OK] をクリックします。

   ACS マシンが再起動します。

   e. ACS 5.8 プライマリ サーバにログインします。

   f. [System Administration] > [Operations] > [Distributed System Management] を選択します。

   g. [Secondary Instances] テーブルから、削除するセカンダリ インスタンスの横にあるチェックボックスをオンにします。

   h. [Delete] をクリックします。

   次のメッセージが表示されます。

   ```
   Are you sure you want to delete the selected item/items?
   ```

   i. [OK] をクリックします。

   [Distributed System Management] ページの [Secondary Instances] テーブルが表示されます。このとき、削除されたセカンダリ インスタンスは表示されません。

3. セカンダリ サーバ データをバックアップします。

   ACS CLI から、EXEC モードで次の **backup** コマンドを発行して、バックアップを実行して、バックアップをリポジトリに入れます。

   backup *backup-name* **repository** *repository-name*

   注:データをバックアップする際、データのサイズが ACS に割り当てられているディスク クォータを超える場合、CLI に警告メッセージが表示され、ACS Monitoring and Reports のアラームが起動します。

4. ACS サーバを 5.8.1 にアップグレードします。ACS サーバの 5.8 から 5.8.1 へのアップグレード（10 ページ）を参照してください。

5. セカンダリ サーバを ACS 5.8.1 プライマリ サーバに登録します。

   a. [System Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

   [Deployment Operations] ページが表示されます。

   b. [Registration] ダイアログボックスの下にある次の必須フィールドに入力します。

   – [Primary Instance]:セカンダリ インスタンスを登録する 5.8.1 プライマリ サーバのホスト名。

   – [Admin Username]:管理者アカウントのユーザ名。

   – [Admin Password]:管理者アカウントのパスワード。

   – [Hardware Replacement]:既存の ACS インスタンスをプライマリ インスタンスに再登録できるようにして、プライマリ インスタンスにすでに存在する設定のコピーを取得する場合にオンにします。

   – [Recovery Keyword]:このセカンダリ サーバが、以前に収集した監視およびレポート データに関連付けられるように、5.8 導入で使用されたものと同じホスト名を指定します。

   この情報の送信後に、このインスタンスはプライマリ インスタンスに接続します。プライマリ インスタンスは、キーワードに基づいて、関連付けられた ACS インスタンス レコードを検索し、各レコードに登録済みのマークを付けます。

   c. [Register to Primary] をクリックします。

   システムに次のメッセージが表示されます。

   ```
   This operation will register this ACS Instance as a secondary to the specified Primary Instance.ACS
   will be restarted.You will be required to login again.Do you wish to continue?
   ```

   d. [OK] をクリックします。

   ACS は自動的に再起動します。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

   注:セカンダリ インスタンスをプライマリ インスタンスに登録する際、プライマリ インスタンスで作成したアカウントはどれでも使用できます。プライマリ インスタンスで作成するクレデンシャルは、セカンダリ インスタンスに複製されます。

   登録の完了後に、ACS によって完全同期が実行され、ACS 5.8.1 構成データが 5.8.1 セカンダリ サーバに送信されます。

6. ローカルおよび未処理の証明書の署名要求（CSR）をインポートします。

   『*User Guide for Cisco Secure Access Control System 5.8.1*』の「Importing Server Certificates and Associating Certificates to Protocols」の項と「Generating Self-Signed Certificates」の項を参照してください。

   プライマリ サーバのアップグレード（8 ページ）に進みます。

すべてのセカンダリ サーバを ACS 5.8.1 にアップグレードしてから、ACS 5.8 プライマリ サーバを ACS 5.8.1 にアップグレードします。プライマリ サーバに登録されたセカンダリ サーバがない場合は、プライマリ サーバ自体がログ コレクタとして機能します。

プライマリ サーバのアップグレード

プライマリ サーバを 5.8 から 5.8.1 導入にアップグレードするには、次の手順を実行します。

1. プライマリ サーバがスタンドアロン サーバであることを確認します。

   a. [System Administration] > [Operations] > [Distributed System Management] の順に選択します。

   [Distributed System Management] ページが表示されます。

   b. [Secondary Instances] テーブルにセカンダリ サーバがリストされているかどうかを確認します。セカンダリ サーバがある場合は、5.8 プライマリ サーバをアップグレードする前に、これらのサーバをアップグレードします。セカンダリ サーバのアップグレード（6 ページ）を参照してください。

2. ACS サーバを 5.8.1 にアップグレードします。ACS サーバの 5.8 から 5.8.1 へのアップグレード（10 ページ）を参照してください。

3. 新しくアップグレードされた 5.8.1 サーバを既存のプライマリ ACS 5.8.1 サーバに登録します。

   a. [System Administration] > [Operations] > [Local Operations] > [Deployment Operations] を選択します。

   [Deployment Operations] ページが表示されます。

   b. [Registration] ダイアログボックスの下にある次の必須フィールドに入力します。

   – [Primary Instance]：セカンダリ インスタンスを登録するプライマリ サーバのホスト名。

   – [Admin Username]：管理者アカウントのユーザ名。

   – [Admin Password]：管理者アカウントのパスワード。

   – [Hardware Replacement]：既存の ACS インスタンスをプライマリ インスタンスに再登録できるようにして、プライマリ インスタンスにすでに存在する設定のコピーを取得する場合にオンにします。

   – [Recovery Keyword]：このサーバが、以前に収集した監視およびレポート データに関連付けられるように、5.8 導入で使用されたものと同じホスト名を指定します。

   この情報の送信後に、このインスタンスはプライマリ インスタンスに接続します。プライマリ インスタンスは、キーワードに基づいて、関連付けられた ACS インスタンス レコードを検索し、各レコードに登録済みのマークを付けます。

   c. [Register to Primary] をクリックします。

   システムに次のメッセージが表示されます。

   ```
   This operation will register this ACS Instance as a secondary to the specified Primary Instance.ACS
   will be restarted.You will be required to login again.Do you wish to continue?
   ```

   d. [OK] をクリックします。

   ACS は自動的に再起動されます。しばらく待ってから、すべてのプロセスが正常に稼働していることを確認します。

   注：セカンダリ インスタンスをプライマリ インスタンスに登録する際、プライマリ インスタンスで作成したアカウントはどれでも使用できます。プライマリ インスタンスで作成するクレデンシャルは、セカンダリ インスタンスに複製されます。

   このインスタンスを ACS 5.8.1 プライマリ サーバとして再度プロモートします。セカンダリ サーバのプライマリへのプロモート（9 ページ）を参照してください。

   これで、ACS 5.8 導入が ACS 5.8.1 導入に完全にアップグレードされました。

セカンダリ サーバのプライマリへのプロモート

1. プライマリ サーバの Web インターフェイスから、[System Administration] > [Operations] > [Distributed System Management] を選択します。

   [Distributed System Management] ページが表示されます。

2. [Secondary Instances] テーブルから、プライマリにプロモートするセカンダリ サーバの横にあるチェックボックスをオンにします。

3. [Promote] をクリックします。

   システムに次のメッセージが表示されます。

   ```
   This operation will promote the selected ACS Instance to become the new Primary Instance.As a
   consequence, the current Primary Instance will be demoted to a Secondary.

   Do you wish to continue?
   ```

4. [OK] をクリックします。

   システムは選択したセカンダリ サーバをプライマリに昇格させて、[Primary Instances] テーブルに移動します。既存のプライマリ サーバは、自動的に [Secondary Instances] テーブルに移動されます。

   登録が完了すると、ACS は完全同期を実行し、新たにプロモートされたプライマリ サーバに ACS 5.8.1 設定データを送信します。

ACS Monitoring and Report Viewer のアップグレード

ACS は、Monitoring and Report Viewer のアップグレードをアップグレード中のサブタスクとして呼び出します。

ACS Monitoring and Report Viewer に使用可能な最大のディスク領域は /opt パーティションの 43% です。

ここでは、次の項目について説明します。

- アップグレード後の Monitoring and Report Viewer データの復元（9 ページ）
- データベースのアップグレード（10 ページ）

ACS View データ アップグレードのステータスをモニタするには、すべてのサーバが稼働した後に ACS Web インターフェイスへログインし、Monitoring and Report Viewer で [Monitoring and Reports] > [Dashboard] を選択します。

アップグレード中、[Monitoring and Reports] ダッシュボードは、ステータス「Data Upgrade in Progress」を表示します。ダッシュボードに表示されるステータスがなければ、アップグレードは正常に完了しています。ACS View アップグレードが失敗すると、ダッシュボードに「Upgrade Failed」のメッセージが表示されます。

アップグレード後の Monitoring and Report Viewer データの復元

5.8.1 へのアップグレード後にバックアップ データを復元すると、変更が検出された場合に、変更は ACS によりデータベースおよびレポートと自動的に同期されます。

データを復元する期間ではなく、バックアップを作成する期間のレポート データだけを使用できます。たとえば、6 月にデータをバックアップし、8 月に復元した場合、使用できるレポート データは 8 月ではなく、6 月のデータになります。最新のレポート データを取得するには、再びレポートを実行する必要があります。

データベースのアップグレード

5.8.1 へのアップグレードの後に、アップグレード以前のバックアップを復元すると、ACS データベースのバージョンは **AVPair:DBVersion=5.8.1** となり、スキーマのバージョンは 5.8.1 に維持されます。データベース プロセスの再開時に、ACS は ACS バージョンとデータベース バージョンを調べて、古いものがあった場合はスキーマとデータのアップグレードを実行します。

ACS 導入の 5.7 から 5.8.1 へのアップグレード

ACS 5.7 の最新パッチをインストールした後、ACS 導入の 5.8 から 5.8.1 へのアップグレード（2 ページ）に示される手順を実施します。

ACS 導入の 5.6 から 5.8.1 へのアップグレード

ACS 5.6 の最新パッチをインストールした後、ACS 導入の 5.8 から 5.8.1 へのアップグレード（2 ページ）に示される手順を実施します。

ACS 導入の 5.5 から 5.8.1 へのアップグレード

ACS 5.5 の最新パッチをインストールした後、ACS 導入の 5.8 から 5.8.1 へのアップグレード（2 ページ）に示される手順を実施します。

ACS サーバの 5.8 から 5.8.1 へのアップグレード

ACS サーバを 5.8 から 5.8.1 にアップグレードする 2 つの方法を次に示します。アップグレードには、次のいずれかの方法を使用できます。

- アプリケーション アップグレード バンドルを使用した ACS サーバのアップグレード（10 ページ）
- ACS サーバの再イメージ化とアップグレード（11 ページ）

アプリケーション アップグレード バンドルを使用した ACS サーバのアップグレード

ACS サーバを 5.8 から 5.8.1 にアップグレードするには、次の手順を実行します。

1. リモート リポジトリに ACS 5.8.1 アプリケーション アップグレード バンドル（ACS_5.8.1.tar.gz）を格納します。

   リポジトリの設定は、『*CLI Reference Guide for Cisco Access Control System 5.8.1*』に示されている手順に従います。

2. EXEC モードで次の application upgrade コマンドを入力します。

   application upgrade ACS_5.8.1.tar.gz *repository-name*

   ACS に、次の確認メッセージが表示されます。

   ```
   Save the current ADE-OS running configuration? (yes/no) [yes]?
   It is strongly recommended to take full backup before upgrade.Do you want to take a backup now?
   (yes/no) [yes]?
   ```

   注：この段階で生成されるバックアップ ファイルは、アプリケーション アップグレード バンドルを保存するために作成された、同じリモート リポジトリに保存されます。

   注：古いバージョンの ACS を 5.8.1 にアップグレードする際、アップグレード バンドルのサイズが割り当てられているディスク クォータを超える場合、CLI に警告メッセージが表示され、ACS Monitoring and Reports のアラームが起動します。

3. **yes** と入力します。

   ACS アップグレードが完了すると、次のメッセージが表示されます。

```
% CARS Install application required post install reboot...
The system is going down for reboot NOW!
Application upgrade successful
```

   ACS は、ACS 5.8 構成データをアップグレードするときに、ACS 5.8 Monitoring and Report Viewer データを 5.8.1 形式に変換します。

4. ACS View データ アップグレードのステータスをモニタするには、すべてのサーバが稼働した後に ACS Web インターフェイスへログインし、Monitoring and Report Viewer で [Monitoring and Reports] > [Dashboard] を選択します。

   アップグレード中、[Monitoring and Reports] ダッシュボードは、ステータス「Data Upgrade in Progress」を表示します。ダッシュボードに表示されるステータスがなければ、アップグレードは正常に完了しています。ACS View アップグレードが失敗すると、ダッシュボードに「Upgrade Failed」のメッセージが表示されます。

5. [OK] をクリックします。

6. **show application version acs** コマンドを入力して、ACS バージョンが正常にアップグレードされたかどうかを確認します。

   次のメッセージが表示されます。

```
Cisco ACS VERSION INFORMATION

-----------------------------

Version : 5.8.1.4
Internal Build ID : B.462
```

7. EXEC モードで **show application status acs** コマンドを入力して、すべてのプロセスが正常に稼働しているかどうかを確認し、Enter を押します。

   コンソールに次のメッセージが表示されます。

```
Process 'database'                  running
Process 'management'                running
Process 'runtime'                   running
Process 'adclient'                  running
Process 'ntpd'                      running
Process 'view-database'             running
Process 'view-jobmanager'           running
Process 'view-alertmanager'         running
Process 'view-collector'            running
Process 'view-logprocessor'         running
```

   これで、すべてのプロセスが稼働し、ACS が正常にバージョン 5.8.1 にアップグレードされたことを確認できました。

ACS サーバの再イメージ化とアップグレード

ここでは、ACS 5.8 のデータをバックアップし、再イメージ化した ACS 5.8.1 サーバに復元することで ACS 5.8 を ACS 5.8.1 にアップグレードする方法について説明します。このアップグレード手順を実行するには、ACS アプライアンスへの物理的なアクセスが必要です。

イメージの再作成と ACS 5.8.1 へのアップグレードを行うには、次の手順を実行します。

1. ACS データを ACS 5.8 サーバからバックアップします。

2. EXEC モードで次の **backup** コマンドを入力して、バックアップを実行し、バックアップをリポジトリに格納します。

   backup *backup-name* **repository** *repository-name*

   注:データをバックアップする際、データのサイズが割り当てられているディスク クォータを超える場合、CLI に警告メッセージが表示され、ACS Monitoring and Reports のアラームが起動します。

   注:ACS 5.8 のデータのバックアップでは、必ずリモート リポジトリを使用します。使用しない場合、5.8.1 インストール後にバックアップしたデータを失うことがあります。

3. ACS 5.8.1 Recovery DVD を使用して ACS 5.8.1 をインストールします。ACS サーバの再イメージ化（6 ページ）を参照してください。

   これにより、構成データなしで ACS サーバのイメージが新しい ACS 5.8.1 サーバに再作成されます。

4. バックアップされたデータを復元する新しい ACS 5.8.1 サーバのリポジトリを設定します。

5. ステップ 2 でバックアップされたデータを ACS 5.8.1 サーバに復元します。

   EXEC モードで **restore** コマンドを入力して、バックアップを復元します。

   restore *filename* **repository** *repository-name*

   注:バックアップされたデータを復元する際、データのサイズが割り当てられているディスク クォータを超える場合、CLI に警告メッセージが表示され、ACS Monitoring and Reports のアラームが起動します。

   注:ADE-OS バックアップを別のハードウェアに復元した場合、確実な動作のためには、ACS マシンの IP アドレスを変更する必要があります。

   5.8 バックアップ ファイルを使用してデータを復元している間に、このコマンドによって ACS 5.8 構成データが復元されます。また、このコマンドによって、ACS 5.8 Monitoring and Report Viewer データが 5.8.1 形式に変換され、アップグレードされます。

   バックアップされたデータ サイズが、ACS で許可されたディスク クォータを超過している場合は、CLI に警告メッセージが表示され、ACS Monitoring and Report にアラームが表示されます。

6. ACS View データ アップグレードのステータスをモニタするには、すべてのサーバが稼働した後に ACS Web インターフェイスへログインし、Monitoring and Report Viewer で [Monitoring and Reports] > [Dashboard] を選択します。

   アップグレード中、[Monitoring and Reports] ダッシュボードは、ステータス「Data Upgrade in Progress」を表示します。ダッシュボードに表示されるステータスがなければ、アップグレードは正常に完了しています。ACS View アップグレードが失敗すると、ダッシュボードに「Upgrade Failed」のメッセージが表示されます。

7. [OK] をクリックします。

警告:**ACS の復元では EAP の PKI や管理インターフェイスは更新されません。データベースに CA 署名付き証明書しかない場合でも、HTTPS は自己署名証明書を使用します。**
この問題の回避策は次のとおりです。
1. 一時的な自己署名証明書を作成し、EAP または管理インターフェイスを割り当てます。
2. EAP または管理インターフェイスを CA 署名付き証明書に再度割り当てます。
3. 自己署名証明書を削除します。

注:バックアップ データのサイズが大きい場合は、抽出プロセスの完了までに 1 時間から数時間かかることがあります。

注:IP の重複の問題を避けるため、同じ ACS サーバ内でバックアップ ファイルを復元します。

ACS サーバの 5.7 から 5.8.1 へのアップグレード

ACS 5.7 サーバを ACS 5.8.1 にアップグレードするには、ACS 5.7 の最新のパッチをインストールし、その後ACS サーバの 5.8 から 5.8.1 へのアップグレード（10 ページ）に示されている手順を実行します。

ACS サーバの 5.6 から 5.8.1 へのアップグレード

ACS 5.6 サーバを ACS 5.8.1 にアップグレードするには、ACS 5.6 の最新のパッチをインストールし、その後ACS サーバの 5.8 から 5.8.1 へのアップグレード（10 ページ）に示されている手順を実行します。

ACS サーバの 5.5 から 5.8.1 へのアップグレード

ACS 5.5 サーバを ACS 5.8.1 にアップグレードするには、ACS 5.6 の最新のパッチをインストールし、その後ACS サーバの 5.8 から 5.8.1 へのアップグレード（10 ページ）に示されている手順を実行します。

ACS パッチの適用

ACS 5.8.1 累積パッチは次の場所からダウンロードできます。

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

注：最新のパッチを使用して ACS 5.8 バージョンから ACS 5.8.1 バージョンにアップグレードする場合、ACS 5.8 パッチの特定の修正が確実に ACS 5.8.1 にも反映されるよう、ACS 5.8.1 に ACS 5.8 パッチをインストールする必要があります。ACS 5.8 パッチは 5.8.1 に適用できます。そのため、ACS 5.8.1 バージョンにも ACS 5.8 パッチをインストールできます。

パッチをダウンロードして適用するには、次の手順を実行します。

1. Cisco.com にログインして、[Security] > [Access Control and Policy] > [Policy and Access Management] > [Cisco Secure Access Control System] > [Cisco Secure Access Control System 5.8.1] に移動します。
2. パッチをダウンロードします。
3. EXEC モードで次の **acs patch** コマンドを実行して、ACS 5.8.1 累積パッチをインストールします。ACS パッチをインストールするには、次の手順を実行します。

   acs patch install *patch-name* **repository** *repository-name*

   ACS に、次の確認メッセージが表示されます。

   ```
   Save the current ADE-OS running configuration? (yes/no) [yes] ? Yes
   ```

   注：古いバージョンの ACS を 5.8.1 にアップグレードする際、アップグレード バンドルのサイズが割り当てられているディスク クォータを超える場合、CLI に警告メッセージが表示され、ACS Monitoring and Reports のアラームが起動します。

4. **yes** と入力します。

   ACS に次のメッセージが表示されます。

   ```
   Generating configuration...
   Saved the ADE-OS running configuration to startup successfully
   Getting bundle to local machine...
     md5: aa45b77465147028301622e4c590cb84
     sha256: 3b7f30d572433c2ad0c4733a1d1fb55cceb62dc1419b03b1b7ca354feb8bbcfa
   % Please confirm above crypto hash with what is posted on download site.
   % Continue? Y/N [Y]?
   ```

5. ACS 5.8.1 パッチのインストールに、MD5 および sha256 チェックサムが表示されます。この値を、ダウンロードされたサイトの Cisco.com で表示される値と比較します。次のいずれかを実行します。

- 暗号ハッシュが一致する場合は、**Y** を入力します。Y を入力すると、ACS はインストール手順を続行します。

```
% Installing an ACS patch requires a restart of ACS services.
Would you like to continue? yes/no
```

- 暗号ハッシュが一致しない場合は、**N** を入力します。N を入力すると、ACS はインストール プロセスを中止します。

6. **yes** と入力します。

   ACS バージョンが、適用されたパッチにアップグレードされます。ACS CLI EXEC モードで

   show application status acs コマンドを使用して、すべてのサービスが正常に実行されていることを確認します。

7. EXEC モードで **show application version acs** コマンドを入力して、パッチが正常にインストールされたことを確認します。ACS に次のメッセージが表示されます。

```
acs/admin# show application version acs

CISCO ACS VERSION INFORMATION

-------------------------------

Version: 5.8.1.4
Internal Build ID: B.462
Patches:
5-8-1-4-1
acs/admin #
```

注: パッチのインストール中、パッチのサイズが割り当てられているディスク クォータを超える場合、ACS CLI に警告メッセージが表示され、ACS Monitoring and Reports ページにアラームが表示されます。

CSACS-1121 上の ACS 5.5、5.6、5.7、5.8 の ACS 5.8.1 使用 Cisco SNS 3400 シリーズ アプライアンスへのアップグレード

CSACS-1121 アプライアンスに ACS 5.5、5.6、5.7、5.8 をインストールしている場合、Cisco SNS-3415 または Cisco SNS-3495 へのアップグレードを行うには、以下の手順を実行します。

1. 既存の ACS 5.5、5.6、5.7、5.8 設定をバックアップします。
2. ACS 5.8.1 がインストールされた Cisco SNS-3415 または Cisco SNS-3495 アプライアンスに ACS をインストールします。
3. ステップ 1 で取得した ACS 5.5、5.6、5.7、5.8 のバックアップを復元します。

注: ACS 5.8.1 を CSACS-1121 から Cisco SNS-3415 または Cisco SNS-3495 アプライアンスに移行する場合、**application upgrade** コマンドは使用できません。Cisco SNS-3415 または Cisco SNS-3495 アプライアンスに ACS 5.8.1 をインストールし、CSACS-1121 アプライアンスからのバックアップを復元する必要があります。

CSACS-1121 または SNS-3400 上の ACS 5.5、5.6、5.7、5.8 の ACS 5.8.1 使用 Cisco SNS 3500 シリーズ アプライアンスへのアップグレード

CSACS-1121、Cisco SNS-3415、または Cisco SNS-3495 アプライアンスに ACS 5.5、5.6、5.7、5.8 をインストールしている場合、Cisco SNS-3515 または Cisco SNS-3595 アプライアンスへのアップグレードを行うには、以下の手順を実行します。

1. 既存の ACS 5.5、5.6、5.7、5.8 設定をバックアップします。
2. ACS 5.8.1 がインストールされた Cisco SNS-3515 または Cisco SNS-3595 アプライアンスに ACS をインストールします。
3. ステップ 1 で取得した ACS 5.5、5.6、5.7、5.8 のバックアップを復元します。

注: ACS 5.8.1 を CSACS-1121、Cisco 3400 シリーズ アプライアンスから Cisco SNS 3500 シリーズ アプライアンスに移行する場合、**application upgrade** コマンドは使用できません。Cisco SNS 3500 シリーズ アプライアンスに ACS 5.8.1 をインストールし、CSACS-1121 または Cisco 3400 シリーズ アプライアンスから取得したバックアップを復元する必要があります。

CSACS-1121 または SNS-3400 上の ACS 5.5、5.6、5.7、5.8 の ACS 5.8.1 使用 Cisco SNS 3500 シリーズ アプライアンスへのアップグレード

インストール後のタスク

インストール後のタスク

この章では、ACS のインストールが正常に完了した後で実行する必要があるタスクについて説明します。

この章の内容は、次のとおりです。

- ライセンス（1 ページ）
- Web インターフェイスへのアクセス（2 ページ）
- ACS の設定（4 ページ）

ライセンス

ACS を使用するには、有効なライセンスをインストールする必要があります。ACS では、初めて Web インターフェイスにアクセスしたときに、有効な基本ライセンスをインストールするよう求められます。

注: 分散導入では、各サーバに固有の基本ライセンスが必要です。

ここでは、次の項目について説明します。

- ライセンスのタイプ（1 ページ）

ライセンスのタイプ

表 1（1 ページ）に、ACS 5.8.1 ライセンスのサポートを示します。

表 1　ACS ライセンスのサポート

ライセンス	説明
ベース ライセンス	基本ライセンスは、導入されているすべてのソフトウェア インスタンスおよびすべてのアプライアンスで必要です。基本ライセンスでは、ライセンス制御された機能を除く ACS のすべての機能を使用でき、標準的な集中化されたレポート機能を有効にできます。 ■ 各 ACS インスタンス（プライマリとセカンダリ）で必要です。 ■ すべてのアプライアンスで必要です。 ■ 最大 500 のネットワーク デバイス（AAA クライアント）を使用した導入をサポートします。 基本ライセンスには次の種類があります。 ■ 永続：このライセンスには有効期限がありません。最大 500 のネットワーク デバイス（AAA クライアント）を使用した導入をサポートします。 ■ 評価：ライセンスを発行してから 90 日後に有効期限が切れます。最大 50 台の管理対象デバイスを使用した導入をサポートしています。 デバイスの数は、設定する一意の IP アドレスの数で決まります。これには、設定するサブネット マスクも含まれます。たとえば、サブネット マスクが 255.255.255.0 の場合、256 個の一意な IP アドレスが提供され、デバイス数は 256 台になります。
アドオン ライセンス	アドオン ライセンスは、永続基本ライセンスがある ACS サーバだけにインストールできます。大規模導入では、永続基本ライセンスをインストールする必要があります。

Web インターフェイスへのアクセス

ACS Web インターフェイスは、HTTPS 対応の Microsoft Internet Explorer および Mozilla Firefox ブラウザでサポートされています。対応ブラウザとバージョンの詳細については、『*Release Notes for Cisco Secure Access Control System 5.8.1*』を参照してください。

ここでは、次の項目について説明します。

- ログイン（2 ページ）
- ログアウト（3 ページ）

ログイン

ACS の Web インターフェイスに初めてログインすると、ライセンス ファイルをインストールするよう求められます。

ACS の Web インターフェイスにログインするには、次の手順を実行します。

1. ブラウザで ACS の URL を入力します。

   たとえば、**https://***acs_host*/**acsadmin, https://[***IPv6 address***]/acsadmin**、または **https://ipv4 address/acsadmin**。acs_host は IP アドレスまたは DNS ホスト名です。IPv6 用の DNS ホスト名が機能するのは、IP アドレスが IPv4 と IPv6 の両方の形式で解決される場合です。

   ログイン ページが表示されます。

注：Mozilla Firefox バージョン 4.x 以降では、IPv6 アドレスを使用する ACS Web インターフェイスの起動はサポートされていません。

2. [Username] フィールドに、デフォルトのユーザ名 **`ACSAdmin`** を入力します。大文字と小文字は区別されません。
3. [Password] フィールドに、デフォルトのパスワード **`default`** を入力します。パスワードでは、大文字と小文字が区別されます。

   注：必要な場合は、[Reset] をクリックすることでユーザ名とパスワードのフィールドをクリアして最初からやり直します。

4. [Login] をクリックするか、Enter を押します。

   ログイン ページが再び表示され、パスワードを変更するよう求められます。

5. [Old Password] フィールドに **`default`** と入力し、[New Password] フィールドと [Confirm Password] フィールドに新しいパスワードを入力します。

   パスワードを忘れた場合、**acs reset-password <*username*>** コマンドを使用して、パスワードをデフォルトの設定にリセットします。リセット後、パスワードを変更するよう求められます。詳細については、『*CLI Reference Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。

6. [Login] をクリックするか、Enter を押します。

   図 1（3 ページ）に示すように、有効なライセンスをインストールするよう求められます。

図 1　ACS 5.8.1 のライセンス画面

ライセンス ページは、初めて ACS にログインするときにだけ表示されます。

7. [Browse] をクリックし、ACS サーバの有効な一意の基本ライセンスを選択します。

   有効なライセンスのインストールの詳細については、『*User Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。

- ログインに成功すると、ACS の Web インターフェイスのメイン ページが表示されます。
- ログインに失敗すると、次のエラー メッセージが表示されます。

  Access Denied. Please contact your system administrator for assistance.

  [Username] フィールドと [Password] フィールドがクリアされます。

8. 有効なユーザ名とパスワードを再度入力し、[Login] をクリックします。

注:ACS Web インターフェイスを表示するために Internet Explorer を使用すると、セキュリティ強化の構成（ESC）が有効な場合、ACS Web インターフェイスのポップアップや表示ページに問題が発生します。この問題を解決するには、Internet Explorer の設定から ESC を無効にする必要があります。

ログアウト

ACS Web インターフェイスからログアウトするには、次の手順を実行します。

1. ACS の Web インターフェイスの見出しで [Logout] をクリックし、管理セッションを終了します。

   ACS からログアウトするかどうかの確認を求めるダイアログボックスが表示されます。

2. [OK] をクリックします。

   ログアウトされました。

注:**セキュリティのため、管理セッションを完了時に ACS からログアウトすることを推奨します。ログアウトしない場合、30 分間何も操作しないと ACS の Web インターフェイスからログアウトされます。このとき、未送信の設定データは保存されません。**

Web インターフェイスの使用の詳細については、『*User Guide for the Cisco Secure Access Control System 5.8.1*』を参照してください。

ACS の設定

初期設定を行うには ACS の Web インターフェイスを使用します。ACS の Web インターフェイスでは、ページへのアクセス、設定作業の実行、インターフェイス設定エラーの確認を行うことができます。

ライセンス ファイルのインストールが終了したら、次の ACS 設定を行います。

- システム管理者とアカウントの設定
- 分散導入での ACS の設定
- 次のシステム管理設定の管理
  - グローバル システム オプションの設定
  - ディクショナリの設定
  - ローカル サーバ証明書の設定
  - ログの設定
- データのバックアップの設定
- 収集フィルタの設定
- ACS ロギングの管理
- E メール設定の指定
- セッション設定の指定
- システム アラーム設定の指定
- データ消去の設定
- パスワード ポリシーの設定

ACS モニタリングやレポートなど、各操作と他の管理機能についての詳細は、『*User Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。

移行の詳細や移行に関する問題については、『*Migration Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。

Cisco.com の最新情報については、『*Release Notes for Cisco Secure Access Control System 5.8.1*』を参照してください。

参照

トラブルシューティング

CSACS-1121、Cisco SNS-3415、Cisco SNS-3495、Cisco SNS-3515、Cisco SNS-3595 シリーズ アプライアンスでは、出荷前に精密なテストを実施しています。問題が発生した場合は、この付録を使用して問題を特定するか、問題の原因であるアプライアンスの使用を停止してください。

初期起動時に過熱または過電圧の状態になることはまれですが、環境の温度や電圧のモニタリング機能については法規制の遵守（6 ページ）の項で解説します。

注: この章の手順では、CSACS-1121 シリーズ、Cisco SNS-3415、Cisco SNS-3495、Cisco SNS-3515、Cisco SNS-3595 シリーズ アプライアンスの初期起動時におけるトラブルシューティングについて、アプライアンスが工場出荷時の設定のままであることを前提に解説します。コンポーネントを削除または交換している、もしくはデフォルト設定を変更している場合は、この章の推奨事項を適用できない場合もあります。

この付録では、アプライアンスに起こりうる問題すべてを網羅するのではなく、お客様で頻繁に確認されている問題を中心に取り上げます。

この付録の内容は、次のとおりです。

- トラブルシューティングの概要（1 ページ）
- 問題解決（2 ページ）
- LED の読み取り方（5 ページ）
- 製品シリアル番号の場所（7 ページ）

トラブルシューティングの概要

初期システム起動時、次の事項を確認します。

- 外部電源コードが接続されており、正しい電源が供給されている。詳細については、電源の考慮事項（8 ページ）、電源仕様（5 ページ）、CSACS-1121 シリーズ アプライアンスの電源投入（17 ページ）、Cisco SNS-3415/3495 アプライアンスの接続と電源投入（10 ページ）、Cisco SNS-3515 または 3595 アプライアンスの接続と電源投入（8 ページ）、および CSACS-1121 シリーズ アプライアンスでの電源および冷却システムのトラブルシューティング（3 ページ）を参照してください。
- アプライアンスのファンとブロワーが稼働している。通気に関するガイドライン（7 ページ）、環境仕様（4 ページ）、および CSACS-1121 シリーズ アプライアンスでの電源および冷却システムのトラブルシューティング（3 ページ）を参照してください。
- アプライアンスのソフトウェアが正常に起動している。
- アダプタ カード（インストールされている場合）がスロット内に正しく設置されており、それぞれが（アプライアンス ソフトウェアによって）問題なく初期化されている。

以上の条件がそれぞれ満たされており、ハードウェアの設置が完了している場合は、基本設定に移ります。正しい設定機能については、第 5 章「CSACS-1121 を使用した Cisco Secure Access Control System のインストールと設定」、第 9 章「Cisco SNS-3415 および Cisco SNS-3495 を使用した Secure Access Control System のインストールと設定」、第 13 章「Cisco SNS-3515 および Cisco SNS-3595 を使用した Secure Access Control System のインストールと設定」、または『*User Guide for Cisco Secure Access Control System 5.8.1*』を参照してください。

問題を特定できない場合は、手順についてカスタマー サービス担当者にお問い合わせください。テクニカル サポートについては、アプライアンスに付属される『*Cisco Information Packet*』を参照してください。お問い合わせいただく前に、次の情報をお手元にご用意ください。

- アプライアンスのシャーシ タイプおよびシリアル番号。詳細については、Cisco Product Identification ツール（3 ページ）を参照してください。
- 保守契約または保証書（『*Cisco Information Packet*』を参照）。
- ソフトウェアのタイプおよびバージョン番号（該当する場合）。
- 新規アプライアンスの入手日。
- 生じている問題の簡単な説明と、問題の特定と解決の手順。

注：カスタマー サービス担当者には、必ず CSACS-1121、Cisco SNS-3415、Cisco SNS-3495、Cisco SNS-3515、Cisco SNS 3595 シリーズ アプライアンスの初期インストール後に行ったアップグレードまたはメンテナンスの情報をすべてお伝えください。サイト ログ情報については、サイト ログの作成（12 ページ）および サイト ログ（1 ページ）を参照してください。

問題解決

問題解決のキーは、CSACS-1121、Cisco SNS-3415、Cisco SNS-3495、Cisco SNS-3515、Cisco SNS-3595 シリーズ アプライアンスの動作と実行されるべき動作とを比較し、問題を特定の箇所に絞り込むことです。

つまり、トラブルシューティングの際は、症状を明確にし、症状を引き起こしうる問題すべてを洗い出してから、症状が消えるまで、その潜在的な問題を（最も起こりやすいものから最も起こりにくいものまで）それぞれ体系的に排除します。

次の手順は、トラブルシューティングのプロセスで活用できるガイドラインです。

1. 問題を分析し、明確に問題を記述したものを作成します。症状と潜在的な原因を定義します。
2. 考えられる原因を特定するのに役立つ事実を収集します。
3. 収集した事実に基づいて考えられる原因を検討します。
4. それらの原因に基づいて処置プランを作成します。最も可能性の高い問題から始め、単一の変数だけを操作するプランを考案します。
5. 実行計画を実施します。各手順を慎重に実行し、症状が消えたか確かめます。
6. 結果を分析し、問題が解決したかどうかを確認します。問題が解決していれば、プロセスは完了です。

   問題が解決していない場合は、リストで次に可能性の高い原因に基づいて処置プランを作成します。4.それらの原因に基づいて処置プランを作成します。最も可能性の高い問題から始め、単一の変数だけを操作するプランを考案します。（2 ページ） に戻り、問題が解決するまでプロセスを繰り返します。

   実行計画を実施するときは、変更した部分を元に戻してください。一度に変更する変数は、1 つだけです。

注：前面パネルと背面パネルの LED から、アプライアンスのパフォーマンスと動作の状態を確認することができます。これら LED の詳細については、LED の読み取り方（5 ページ）を参照してください。

トラブルシューティングの際は、まず、次に示すアプライアンスのサブシステムを確認してください。

- 電源および冷却システム（外部電源、電源ケーブル、アプライアンス ファン）。また、不十分な通気、換気、または環境条件も確認します。
- アダプタ カード。アダプタ カードの LED を確認することで、障害を検知できます。
- ケーブル。アプライアンスをネットワークに接続している外部ケーブルがすべてしっかり装着されているかを確認します。

CSACS-1121 シリーズ アプライアンスでの電源および冷却システムのトラブルシューティング

電源 LED およびファンのいずれも、電源の問題のトラブルシューティングを行う際に役立ちます。次の項目を確認し、問題を特定します。

- CSACS-1121 シリーズ アプライアンスが電源に接続されているとき、アプライアンスの前面パネルにある電源 LED が点灯しているかを確認します。点灯していない場合、AC 電源コードの接続を確認します。それでも電源 LED が消灯している場合は、電源に障害が発生している可能性があります。
- アプライアンスがオンになっても、すぐにシャットダウンする場合は、
  - 環境によって引き起こされるシャットダウンの可能性を検証します。詳細については、環境レポート機能（3 ページ）の項を参照してください。
  - ファンを確認します。ファンが動作していない場合、アプライアンスは過熱されて自動的にシャットダウンします。

  ファンが動作していないのであれば、ファンの電源接続を確認します。

  電源接続を確認する際は、アプライアンスをシャットダウンして外部ケーブルを取り除いてから、アプライアンスを開けます。
  - アプライアンスの吸気口と排気口に何もないことを確認してください。
  - 環境に関連する設置場所の要件については、温度と湿度に関するガイドライン（8 ページ）を参照してください。
- アプライアンスの一部は起動しても、LED が点灯しない場合は、アプライアンスの前面パネルにある電源 LED を確認して電源障害の有無を確認します。
  - LED が点灯している場合は、電源は機能しています。
  - LED が点灯していない場合は、『*Cisco Information Packet*』で保証情報を確認するか、カスタマー サービス担当者にお問い合わせください。

環境レポート機能

CSACS-1121 シリーズ アプライアンスは、アプライアンス内部の過電流、過電圧、過熱の状態をモニタリングして検出する保護回線を備えています。

電源がシャットダウンまたは停止状態になった場合、AC サイクルは 15 秒間オフの状態になってから、1 秒間オンの状態になって電源をリセットします。詳細については、法規制の遵守（6 ページ）を参照してください。

次の条件によって、アプライアンスが異常な高温状態になる可能性があります。

- ファン障害
- 室内の空調機器の故障
- 冷却ベントへの通気の阻害

問題は手順を追って解決します。環境における動作条件の情報については、温度と湿度に関するガイドライン（8 ページ）を参照してください。

CSACS-1121 シリーズ アプライアンスでのアダプタ カード、ケーブル、接続のトラブルシューティング

ネットワーク障害は、アダプタ カード、ケーブルまたはケーブル接続、もしくはハブやウォール ジャック、WAN インターフェイス、ターミナルなどの外部デバイスが原因になることがあります。次の症状を確認して、問題を特定します。

- CSACS-1121 シリーズ アプライアンスがアダプタ カードを認識しない。
  - アダプタ カードがスロット内に確実に挿入されているかを確認します。
  - アダプタ カードの LED を確認します。各アダプタ カードにはそれぞれ固有の LED のセットが当てられています。
  - ソフトウェア リリースがアダプタ カードをサポートしているかを確認します。アダプタ カード付属の資料を参照してください。
- アダプタ カードは認識されるが、インターフェイス ポートが初期化されない。
  - アダプタ カードがスロット内に確実に挿入されているかを確認します。
  - 外部ケーブルの接続を確認します。
  - ソフトウェア リリースがアダプタ カードをサポートしているかを確認します。アダプタ カード付属の資料を参照してください。
- CSACS-1121 シリーズ アプライアンスが正常に起動しない、または常時もしくは断続的に再起動する。
  - アダプタ カードがスロット内に確実に挿入されているかを確認します。
  - アプライアンス シャーシまたはアプリケーション ソフトウェアを確認します。保証情報については、アプライアンスに付属の『*Cisco Information Packet*』マニュアルを参照するか、カスタマー サービス担当者にお問い合わせください。
- ターミナルでコンソール ポートを使用しており、CSACS-1121 シリーズ アプライアンスが起動してもコンソール画面がフリーズする。
  - 外部コンソールの接続を確認します。
  - ターミナルのパラメータが次のとおり設定されていることを確認します。
    a. ターミナルのデータ レートはアプライアンスと同じにする（デフォルトは 9600 bps）。
    b. 8 データ ビット。
    c. パリティ生成やパリティ チェックが実行されていない。
    d. 1 ストップ ビット。
- CSACS-1121 シリーズ アプライアンスでは、アダプタ カードが取り除かれた場合にだけ、電源がオンになり、起動します。アダプタ カードを確認してください。保証情報については、アプライアンスに付属の『*Cisco Information Packet*』マニュアルを参照するか、カスタマー サービス担当者にお問い合わせください。
- CSACS-1121 シリーズ アプライアンスでは、特定のケーブルが切断された場合にだけ、電源がオンになり、起動します。ケーブルに問題がある可能性があります。保証情報については、アプライアンスに付属の『*Cisco Information Packet*』マニュアルを参照するか、カスタマー サービス担当者にお問い合わせください。

Cisco SNS-3415/3495 アプライアンスの保守

Cisco SNS-3415 または Cisco SNS-3495 アプライアンスは、Cisco UCS C220 サーバに基づいています。Cisco SNS-3415 または Cisco SNS-3495 アプライアンスの保守方法、サーバ コンポーネントの取り付けおよび取り外し方法（必要な場合）については、『Cisco UCS C220 Server Installation and Service Guide』を参照してください。

LED の読み取り方

CSACS-1121、Cisco SNS-3415、および Cisco SNS-3495 アプライアンスには、いくつかの LED が付いています。LED は、次の役割を果たします。

- アプライアンスで利用可能な基本電源を示す。
- ハードディスク、CD ドライブ、ネットワーク アクティビティ状態を示す。

ここでは、次の項目について説明します。

- CSACS-1121 シリーズ アプライアンスの LED（5 ページ）
- Cisco SNS-3415/3495 アプライアンスの LED（7 ページ）

Cisco SNS-3515/3595 アプライアンスの保守

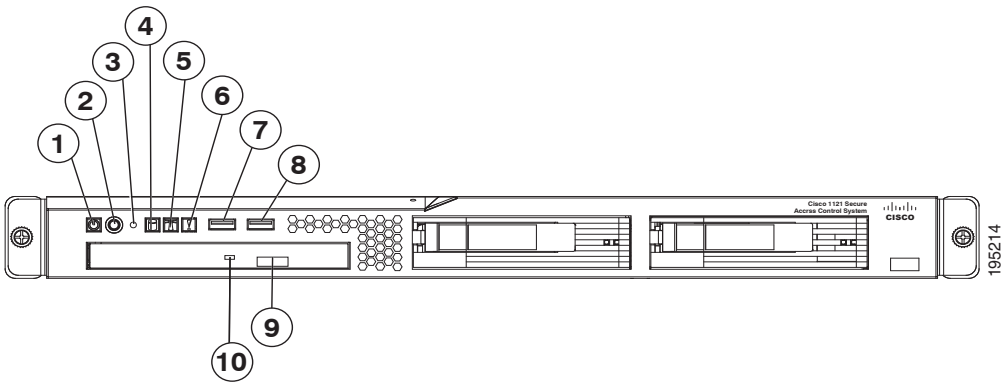
注意：問題の発生を防ぐため、この章の手順を実行する前に安全上の警告（6 ページ）と安全に関する注意事項（1 ページ）のセクションを確認してください。

Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの保守については、『*Cisco UCS C220 M4 Server Installation and Service Guide*』の「Maintaining the Server」の章を参照してください。

CSACS-1121 シリーズ アプライアンスの LED

前面パネルの LED

図 1　　前面パネルの LED



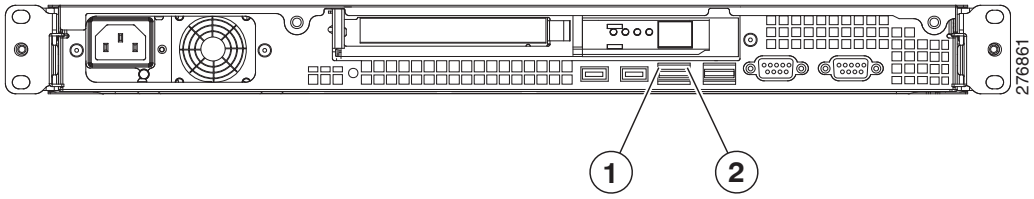
1	アプライアンス電源 LED	6	システム エラー LED
2	電源制御ボタン	7	USB 1 コネクタ
3	リセットボタン	8	USB 2 コネクタ
4	ハードディスク ドライブ アクティビティ LED	9	CD 取り出しボタン
5	ロケータ LED	10	CD ドライブ アクティビティ LED

表 1　　前面パネルの LED の説明

LED	カラー	状態	説明
アプライアンス電源	グリーン	オン	電源がオンです。
	グリーン	点滅	スリープ（スタンバイ）状態です。
	オフ	オフ	電源がオフです。
ハードディスク ドライブ アクティビティ	グリーン	ランダムに点滅	ハードディスク ドライブ アクティビティがあります。
	オフ	オフ	ハードディスク ドライブ アクティビティがありません。
リセットボタン	–	–	このボタンを押すと、ソフト リセットを実行します。
ロケータ LED	青	点滅	システムが起動中です。
	オフ	（Off）	システムの起動が完了しました。
システム エラー	オレンジ	オン	システム エラーが発生しました。
CD ドライブ アクティビティ	グリーン	オン	CD ドライブは使用中です。

背面パネルの LED

図 2　　CSACS-1121 の背面パネルの LED



1	イーサネット アクティビティ LED	2	イーサネット リンク LED

表 2　　背面パネルの LED

LED	カラー	状態	説明
イーサネット アクティビティ LED	グリーン	オン	サーバとネットワーク間でアクティビティがあります。
	グリーン	点滅	サーバとネットワーク間でアクティビティがあります。
	オフ	オフ	アクティビティがありません。
イーサネット リンク LED	グリーン	ランダムに点滅	イーサネット コントローラがネットワークに接続されています。
	オフ	オフ	イーサネット コントローラがネットワークに接続されていません。

Cisco SNS-3415/3495 アプライアンスの LED

Cisco SNS-3415 または Cisco SNS-3495 アプライアンスで使用可能な前面パネル LED を表示するには、Cisco SNS-3415/3495 アプライアンスの前面パネル ビュー（5 ページ）を参照してください。

Cisco SNS-3415 または Cisco SNS-3495 アプライアンスで使用可能な背面パネル LED を表示するには、Cisco SNS-3415/3495 アプライアンスの背面パネル ビュー（6 ページ）を参照してください。

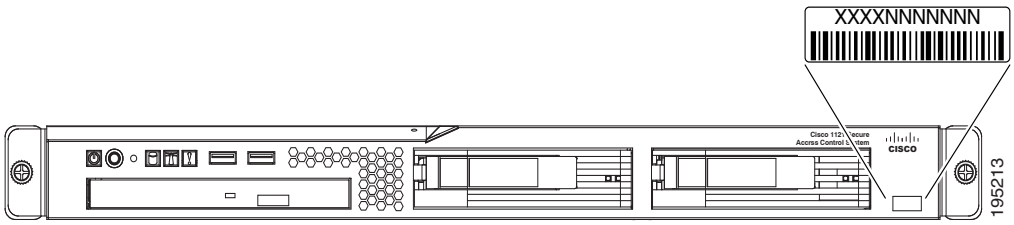
Cisco SNS-3415 または Cisco SNS-3495 アプライアンスで使用可能な内部診断 LED を表示するには、内部診断 LED（7 ページ）を参照してください。

製品シリアル番号の場所

CSACS-1121 シリーズ アプライアンスにおいて、シリアル番号ラベルはアプライアンスの前面パネルの左下にあります。図 3（7 ページ） に、シリアル番号ラベルの場所を示します。

ここでは、Cisco Product Identification ツール（7 ページ）に関する詳細を説明します。

図 3　　CSACS-1121 シリーズ アプライアンスのシリアル番号の場所



注:CSACS-1121 シリーズ アプライアンスのシリアル番号は 11 文字です。

SNS-3415 または SNS-3495 アプライアンスでは、サーバのシリアル番号が前面付近にあるサーバの上部のラベルに印刷されています。

Cisco Product Identification ツール

Cisco 製品 ID（CPI）ツールは、シスコ製品のシリアル番号を取得する際に役立ちます。

オンラインまたは電話でサービスのリクエスト要求をする前に、CPI ツールを使用して製品のシリアル番号を検索します。このツールは、シスコのサポート Web サイトからアクセスできます。

CPI ツールにアクセスする方法は、次のとおりです。

1. [Tools & Resources] リンクをクリックします。
2. [Show All Tools] タブをクリックします。
3. アルファベット順の一覧から [Cisco Product Identification Tool] を選択します。

   このツールには、3 つの検索オプションがあります。

- 製品 ID またはモデル名による検索。
- シスコ モデルの参照。
- **show** コマンドで出力をコピー アンド ペーストして製品を特定。

  検索結果では、製品画像とともにシリアル番号ラベルの場所が強調表示されます。製品のシリアル番号ラベルのある場所を探し、サービスに問い合わせる前にその情報を記録します。

CPI ツールは、Cisco.com の次の URL からアクセスできます。

http://tools.cisco.com/Support/CPI/index.do

シスコ サポートの Web サイトから CPI ツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

サイト ログ

サイト ログは、CSACS-1121 シリーズ アプライアンスのインストールおよび保守に関連するすべてのアクションを記録するものです。タスクを実行する誰もが使用できるよう、ログはアクセスしやすいアプライアンス シャーシの近くに置いてください。インストレーション チェックリスト（インストレーション チェックリスト（12 ページ）を参照）を使用して、アプライアンスのインストールおよび保守の手順を確認します。

サイト ログ エントリには、次の項目が含まれていることがあります。

- 設置の進行：アプライアンスのインストレーション チェックリストのコピーを作成して、サイト ログに挿入します。各タスクの完了時に、エントリを作成します。
- アップグレード、取り外し、およびメンテナンス手順：進行中のアプライアンスのメンテナンスと拡張履歴のレコードとして、サイト ログを使用します。アプライアンスでタスクを実行するたびに、サイト ログを更新して、次の情報を反映させます。
  - 設定変更
  - メンテナンスのスケジュールと要件
  - 実行したメンテナンス手順
  - 間欠的な問題
  - コメントとメモ

表 1（1 ページ） に、サイト ログのサンプルを示します。サンプルをコピーするか、またはサイトおよび機器のニーズに合った独自のサイト ログを設計します。

表 1　サイト ログ

日付	実行したアクションまたは発生した現象の説明	イニシャル
日付	説明	
日付	説明	
日付	説明	

CSACS-1121、Cisco SNS-3400 シリーズ、および Cisco SNS-3500 シリーズ アプライアンスの保守

CSACS-1121、Cisco SNS-3415、Cisco SNS-3495 シリーズ アプライアンスは、注文時に設定でき、インストールできる状態で工場から出荷されます。アプライアンスのインストールおよび設定後、アプライアンスが正常に稼働することを確認するため、特定の保守手順や操作を実行する必要がある場合もあります。

こうした予防手順は、アプライアンスの正常稼働を維持し、コストがかかる上に時間のかかるサービス手順を最小限に抑えることができます。

注意：問題の発生を防ぐため、この章の手順を実行する前に安全上の警告（6 ページ）と安全に関するガイドライン（1 ページ）のセクションを確認してください。

次の項では、アプライアンスのパフォーマンスや寿命に悪影響を与える可能性のあるさまざまな環境要因について説明します。この項では、次の内容について説明します。

- CSACS-1121 シリーズ アプライアンスの保守（1 ページ）
- Cisco SNS-3415/3495 アプライアンスの保守（5 ページ）

CSACS-1121 シリーズ アプライアンスの保守

サイト環境の保守

適切な予防保守とは、外面の清掃や検査など、定期的に目視でアプライアンスを検査することです。

この章の内容は、次のとおりです。

- 一般的な外面清掃と検査（2 ページ）
- 冷却（2 ページ）
- 温度（3 ページ）
- 湿度（3 ページ）
- 高度（3 ページ）
- 静電放電（4 ページ）
- 電磁波干渉および無線周波数干渉（4 ページ）
- 磁気（4 ページ）
- 電源の中断（4 ページ）

一般的な外面清掃と検査

この項では、アプライアンスの外面清掃の要件について説明します。また、ケーブルおよびアダプタ カードの検査についても説明します。

注意：アプライアンスの表面に洗浄液を吹きかけないでください。スプレーのしぶきがアプライアンス内部に入り、電気的な問題や腐食の原因となる場合があります。

アプライアンス

研磨剤が入っていない、表面を削らない柔らかい布で清掃します。溶剤、研磨剤入りの洗浄剤、およびティッシュ ペーパーは*使用しないでください*。アプライアンスが（大量の埃などで）汚れている場合は、湿らせた柔らかい布でアプライアンスの表面をやさしく拭きとります。

水や液体は、すぐに拭きとってください。

埃と微粒子

稼働環境が清潔であれば、埃やその他の微粒子による悪影響を大幅に減らすことができます。埃や微粒子は絶縁体として作用したり、アプライアンスの機械コンポーネントの動作を妨害したりすることがあります。定期的な清掃に加えて、アプライアンスの汚れを防ぐために、次のガイドラインを実施してください。

- アプライアンスの近くでの喫煙を禁止する。
- アプライアンスの近くでの飲食を禁止する。

ケーブルとコネクタ

アプライアンスに*接続されている*ケーブルとコネクタを定期的に検査し、摩耗していたり緩んでいたりしないかを確認します。

アダプタ カード

アダプタ カードの接続を確認します。アプライアンスにアダプタ カードがしっかり装着されており、緩んだり機械的に損傷していたりしないかを確認してください。

腐食

人の指の皮脂や、高温または多湿の環境に長時間さらされると、アプライアンス上のアダプタ カードの金メッキされたエッジ コネクタやピン コネクタが腐食する可能性があります。こうした腐食がアダプタ カードのコネクタで発生すると、腐食が徐々に進んで、最終的には電気回路が断続的に障害を起こす事態へと発展する場合があります。

腐食を防ぐため、アダプタ カードの端子には触れないでください。湿気や塩分の多い環境では腐食が進みやすいため、腐食要素からアプライアンスを保護することは特に重要となります。また、腐食を防止する方法として、温度（3 ページ）の項にあるとおり、極端に温度差のある環境でアプライアンスを使用しないことも必要です。

冷却

電源装置内およびアプライアンス内の排気ファンは、アプライアンスの前面にあるいくつかの開口部分から空気を吸い込んで背面から吐き出すことで、電源装置とアプライアンスを冷却します。

ただし、ファンは埃やその他の微粒子もアプライアンス内に取り込みます。この結果、汚れが蓄積され、アプライアンスの内部温度が上昇し、アプライアンスのさまざまなコンポーネントの動作に影響がでます。

このような状況を回避するには、作業環境を清潔に保ち、アプライアンス周辺の埃や汚れの量を減らし、ファンによってアプライアンス内に引き込まれる汚染源を減らすことを推奨します。

温度

極端な温度差は、集積回路（IC）の経年劣化の促進や障害、またはデバイスの機械的な故障など、さまざまな障害の原因となります。極端な温度変動によってソケット内の IC が緩むと、ディスク ドライブ プラッタでは膨張収縮が起こり、データの読み取りエラーや書き込みエラーが発生する可能性があります。

ACS アプライアンスの熱放射の範囲は、100 ～ 300 W（341 ～ 1024 BTU）です。

温度によってアプライアンスのパフォーマンスが受ける悪影響を最小限に抑えるため、次のガイドラインに従ってください。

- 表 1（ 3 ページ）に、ACS サーバの設置場所の高度に基づき、維持されるべき気温を示します。

表 1　気温のメンテナンス

サーバの状態	高度	気温
オン	3000 フィート（0 ～ 914.4 m）	50.0° ～ 95.0°F（10° ～ 35°C）
オン	3000（914.4 m）～ 7000 フィート（2133.6 m）	50.0° ～ 89.6°F（10° ～ 32°C）
オフ	最大高度：7000 フィート（2133.6 m）	50.0° ～ 109.4°F（10° ～ 43°C）
出荷	最大高度：7000 フィート（2133.6 m）	-40° ～ 140°F（40° ～ 60°C）

- アプライアンスの換気が適切であることを確認してください。閉鎖型の壁面ユニット内や布の上にアプライアンスを設置しないでください。熱がこもる原因となります。直射日光があたる場所にアプライアンスを置くことは避けてください（特に午後）。冬場の暖房の吹き出し口を含め、あらゆる種類の熱源の横に設置しないでください。

高地では、特に適切な換気が重要となります。標高の高い場所のほか、高温の環境でアプライアンスを稼働させる場合も最適なパフォーマンスが得られない可能性があります。このような環境の場合、次の手順に従ってください。

- アプライアンスのすべてのスロットおよび開口部で、特にアプライアンス背面にあるファンの吹き出し口が塞がれていないことを確認する。
- 定期的にアプライアンスを掃除して、過熱の原因にもなる埃やゴミの蓄積を防ぐ。
- アプライアンスが異常な低温にさらされた場合、2 時間のウォームアップ時間をとって、通常の動作温度になってから電源を入れる。これを実施しないと、内部コンポーネント、特にハードディスク ドライブが損傷する可能性があります。

湿度

湿度が高いと、湿気がアプライアンス内まで浸透する可能性があります。この湿気が原因で、内部コンポーネントの腐食と、電気抵抗、熱伝導性、物理的強度、サイズなどの特性の劣化が起こることがあります。アプライアンス内に湿気が充満してくると、ショートが発生し、アプライアンスに甚大な被害を与える可能性があります。

各アプライアンスは、相対湿度 8 ～ 80 %、1 時間あたり 10 % の湿度変化で動作するよう規定されています。温暖期には冷房で、寒冷期には暖房で室温が管理されているビル内では、一般的にアプライアンスが許容できる湿度が維持されます。

ただし、異常に湿度の高い場所にアプライアンスが設置されている場合は、除湿機で許容範囲内の湿度に保ってください。

高度

高度の高い（低気圧の）場所でアプライアンスを稼働させると、強制対流冷却の効率が低下し、アーク放電やコロナ放電などの電気障害の原因になります。また、このような状況では、電解コンデンサなどの、内部圧力がかかっている密閉コンポーネントが動作しなかったり、その効率が低下したりする場合もあります。

静電放電

静電放電（ESD）は、人体やその他の特定の物質に静電気が蓄積することで発生します。通常、この静電気はカーペットの上を歩くなどの単純な動作で発生します。

静電放電は、静電気が放電する現象です。帯電した人がアプライアンスのコンポーネントに触れることで発生します。こうした静電放電は、特に IC などのコンポーネント故障の原因になります。特に相対湿度が 50 % 未満の乾燥した環境で、静電放電は問題となります。

静電放電の影響を軽減するには、次のガイドラインに従ってください。

- 静電気防止用リスト ストラップを着用する。静電気防止用リスト ストラップが用意できない場合、定期的にアプライアンスの非塗装金属面に触れて静電気を逃がす。
- コンポーネントは取り付けまで静電気防止パッケージから取り出さない。
- ウールまたは合成繊維の衣服を着用しない。

電磁波干渉および無線周波数干渉

アプライアンスからの電磁波干渉（EMI）および無線周波数干渉（RFI）は、アプライアンスの近くで稼働しているラジオやテレビの受信機などのデバイスに悪影響を与える可能性があります。また、アプライアンスから放出される無線周波数がコードレス電話や低出力の電話に影響をおよぼすこともあります。

RFI は、10 kHz を超える周波数を発生させる EMI として定義されます。この種の干渉は、電源ケーブルや電源、または無線電波のように空気を介して、アプライアンスから他のデバイスへと伝播します。米国連邦通信委員会（FCC）は、コンピュータ装置が放出する EMI および RFI の量を制限する固有の規制を公表しています。各アプライアンスは、これら FCC の規制に準拠します。

EMI および RFI の発生を抑えるために、次の注意事項に従ってください。

- 必ずカバーを取り付けた状態でアプライアンスを稼働する。
- すべての周辺ケーブル コネクタのネジがアプライアンス背面の対応するコネクタにしっかりと取り付けられていることを確認する。
- アプライアンスに周辺機器を接続する際は、必ず金属製のコネクタ シェル付きシールド ケーブルを使用する。

磁気

ハードディスク ドライブはデータを磁気で記憶するため、磁気の影響を受けやすくなっています。ハードディスク ドライブは、次のような磁気を発生させるもののそばに保管しないでください。

- モニタ
- プリンタ
- リアル ベル付きの電話機
- 蛍光灯

電源の中断

アプライアンスは、特に AC 電源から供給される電圧の変動の影響を受けやすくなっています。過電圧、低電圧、過渡電流（またはスパイク）は、メモリからデータを消去するだけでなく、コンポーネントの障害を発生させることもあります。このような種類の問題からアプライアンスを保護するには、電源ケーブルを常に正しく接地し、次のいずれかの方法、または両方の方法を使用します。

- アプライアンスを専用の電力回路に設置する（他の電気機器と回路を共有させない）。一般的に、アプライアンスの電力回路を次の装置と共有させないこと。
  - コピー機
  - テレタイプ
  - レーザー プリンタ
  - ファクス機
  - その他の電動装置

上記の装置以外で、アプライアンスの電源に対する最大の脅威は、落雷によるサージまたは停電です。

アプライアンスに電源が入っているときに停電が発生した場合、停電が一時的なものであったとしても、すぐにアプライアンスの電源を切り、電源コードから外してください。アプライアンスを接続したままにしていると、電力が復旧した際に問題が発生する可能性があります。

Cisco SNS-3415/3495 アプライアンスの保守

注意：問題の発生を防ぐため、この章の手順を実行する前に安全上の警告（6 ページ）と安全に関する注意事項（1 ページ）のセクションを確認してください。

Cisco SNS-3415 および Cisco SNS-3495 アプライアンスを保守するには、『*Cisco UCS C220 M3 Server Installation and Service Guide*』の「Maintaining the Server」の章を参照してください。

Cisco SNS-3515/3595 アプライアンスの保守

注意：問題の発生を防ぐため、この章の手順を実行する前に安全上の警告（6 ページ）と安全に関する注意事項（1 ページ）のセクションを確認してください。

Cisco SNS-3515 または Cisco SNS-3595 アプライアンスの保守については、『*Cisco UCS C220 M4 Server Installation and Service Guide*』の「Maintaining the Server」の章を参照してください。