

ユーザーガイド

Avigilon ACC™ ES HD レコーダー

VMA-RPO-4P2 および VMA-RPO-4P4

© 2015年 - 2020, Avigilon Corporation. 無断複写・複製・転載禁止。AVIGILON、AVIGILONロゴ、AVIGILON CONTROL CENTER、およびACCは、Avigilon Corporationの商標です。MAC、MacOS、FINDERおよびMACINTOSHはApple Inc.の登録商標です。FIREFOXはMozilla Foundationの登録商標です。Androidは、Google LLCの商標です。本書に記載されたその他の名称またはロゴは、該当する所有者の商標である可能性があります。本書で、商標の横に™ および® の記号がない場合でも、該当する商標の所有権を放棄してはおりませんので、予めご了承ください。Avigilon Corporationは、アメリカ合衆国およびその他の世界中にある管轄区域で発行された特許をもって、新技術を保護します (avigilon.com/patentsを参照)。書面で明示的に付与されない限り、Avigilon Corporation またはそのライセンサーの著作権、工業デザイン、商標、特許またはその他の知的財産権の使用は許可されません。

本文書は、本文書が公開された時点での製品情報と仕様を編集および公開したものです。本文書の内容と文書内で説明されている製品の仕様は事前の通知無く変更されることがあります。Avigilon Corporationは、予告なくそのような変更を行う権限を有します。Avigilon Corporation やその関連会社は：（1）この文書の情報の完全性もしくは正確性を保証することはありません。（2）この情報の利用や信頼について責任を負うものではありません。Avigilonは、本書内の情報を信頼したことによるいかなる損害（間接損害を含む）にも責任を負うものではありません。

Avigilon Corporation
avigilon.com

PDF-4Port-B

改訂：2 - JA

20200706

このデバイスには、バッテリー駆動のリアルタイムクロック (RTC) 回路が付属しています。RCTバッテリーの交換を正しく行わないと、爆発する危険があります。メーカー推奨、または同等の種類を交換してください。使用済みバッテリーは、メーカーの指示に従って廃棄してください。

本機器は、工場外にルーティングされていないPoE ネットワークにのみ接続します。

目次

はじめに	1
始める前に	1
パッケージの内容	1
概要	2
正面図	2
後ろから見たところ	2
システム要件	3
サポート対象のネットワーク構成	4
初回のACC ES HD レコーダーの起動	5
レコーダーの設定	8
ACC ES管理者Web UIの起動	8
PoEポートのステータスの表示	10
ACCサービスとストレージの管理	11
サポートのためのサービスログの提供	12
デバイスの再起動とデバイス設定の管理	12
ストレージドライブの状態の監視	14
デバイスをユーザーとカメラに接続する	15
PoE 電源予算の割り当て	16
サポートのためのデバイスログの提供	17
ACC Client のインストールと起動	19
ACC ソフトウェアとACS への接続	20
ACC ソフトウェアのアクティブ化と構成	20
Avigilonクラウド サービスへの接続	20
ACC クライアントソフトウェアのスタートアップとシャットダウン	20
外部デバイスへの接続	21
LED インジケータ	22
フロントパネルのLED	22
バックパネルのLED	23
PoE 電源への電力配分	24
証明書の管理	25

Web 証明書の交換	26
信頼できるCA証明書をアップロードする	27
ファームウェアのアップグレード	29
リセット ボタンの使用	31
システムの再起動	31
工場出荷時の設定への復元	31
トラブルシューティング	33
デバイスを検出できません	33
ネットワーク構成	34
システム正常性のチェック	34
詳細について	35
技術サポート	35
アップグレード	35
フィードバック	35

はじめに

Avigilon ACC ES HD レコーダーは、ネットワークビデオ録画のための一体型ソリューションです。このレコーダーには次の機能があります。

- IP カメラを接続し、電力を供給するネットワークスイッチ。
- Avigilon Control Center サーバー ソフトウェアを実行するための内蔵サーバー。
- リモートでアクセスできるローカル ビデオ コンテンツ ストレージ。

ACC ES HD レコーダー の工場出荷時の設定を使用すると、レコーダー設置後すぐに使用を開始できますが、特殊な要件などがある場合は、Avigilon Control Center ソフトウェアまたは Web インターフェイスを使用して設定をカスタマイズできます。

始める前に

Avigilonビデオ監視システムのハードウェアを保護するために、無停電電源装置（UPS）システムの使用をお勧めします。UPSシステムは、専用バッテリーを使用して、スパイク、電圧低下、変動、および完全な電源障害などの主電源の問題から重要な機器を保護するために使用されます。スタンバイ発電機を始動し同期させるのにかかる時間中に機器に電力を供給するためにも使用できます。

どのUPS接続にも、バッテリー残量が少ないか、15分の電力しか残っていない場合にアプライアンスのオペレーティングシステムをシャットダウンする設定を含める必要があります。

適切なネットワーク構成を設定するまで、カメラをアプライアンスに接続しないでください。

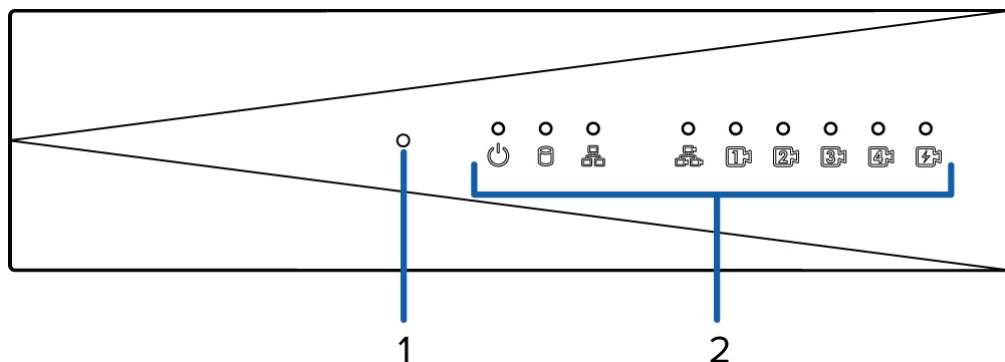
パッケージの内容

パッケージに次のものが同梱されていることを確認してください。

- Avigilon ビデオ アプライアンス
- 電源コード
- 電源装置とそれを固定するためのドライバー
- 壁面取り付け用ハードウェア
- デジタル入出力端子台コネクタ

概要

正面図



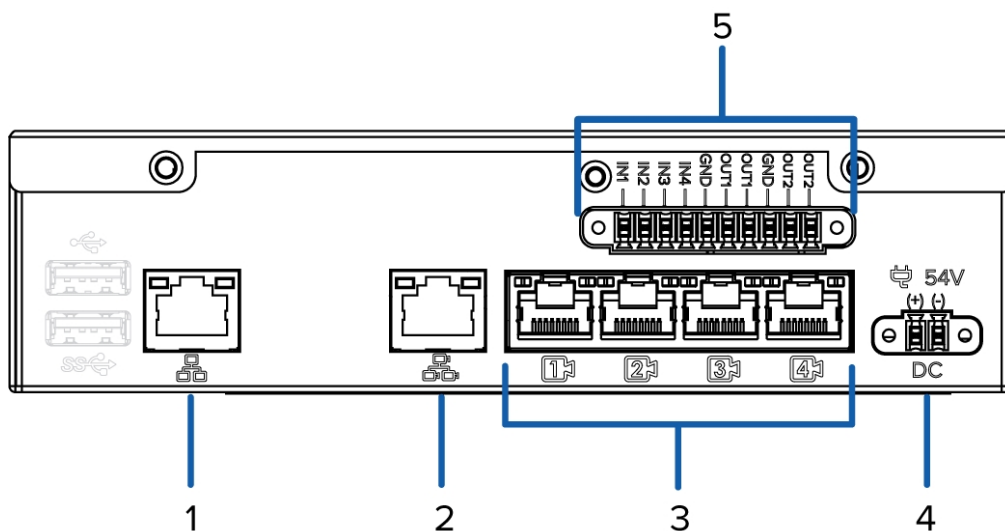
1. リセット ボタン

このボタンを使用して、物理的にレコーダーを再起動したり、工場出荷時の設定にリセットしたりします。

2. ステータス LED

毎日の動作に関する情報を提供します。詳細については、「「LED インジケーター」 (22ページ)」を参照してください。

後ろから見たところ



1. 企業ネットワーク アップリンクポート

1GbE イーサネット接続で汎用ネットワークに接続して、ユーザーが Web インターフェイスや接続済みのカメラビデオにアクセスできるようにします。

2. カメラ ネットワーク アップリンクポート

1GbE イーサネット接続で、PoE スイッチ コンポーネントに接続されているカメラに接続できるようにします。他の PoE スイッチやカメラへのリンクとして使用できます。

3. PoE スイッチ コンポーネント

カメラを 10/100速度の PoE スイッチ コンポーネントに接続して、カメラに電力を供給したりビデオを録画したりします。

4. 電源コネクタ

レコーダーに対する電源を受け入れます。

5. I/O コネクタ

外部の入力/出力デバイスへの接続を提供します。詳細については、「外部デバイスへの接続」(21ページ)を参照してください。

システム要件

アプライアンスの管理設定は、次のいずれかのWebブラウザを使用して、任意のWindows、Mac、またはモバイルデバイスからアクセスされるWebインタフェースを介して管理されます。

- Mozilla Firefoxブラウザバージョン 3.6 以降
- Google Chrome ブラウザ 8.0 以降
- Microsoft Edge ブラウザ 25 以降
- Safari 5.0 以降
- Android 版 Chrome 2.2 以降
- Apple iOS 版 Safari 5 以降
- Windows Internet Explorer ブラウザバージョン 7.0 以降

メモ： Web ブラウザでクッキーを許可するように設定しておかないと、Web インターフェイスは正しく機能しません。

サポート対象のネットワーク構成

メモ：カメラのアップリンクポートでは動的切替えの DHCP サーバーをサポートしていません。

ネットワーク 接続	カメラの Web インターフェ イスアクセス	サポート対象の IP 構成		メモ
		企業の LAN アップリンク	カメラの LAN アップリンク	
企業の LAN アップリンク 専用	なし	静的/DHCP の割り 当て	未接続 (DHCP として残 す)	カメラの LAN アップリンクと 接続済みカメラは Zeroconf IP アドレスを使用します。
カメラの LAN アップリンク 専用	あり	未接続 (DHCP として残 す)	静的、DHCP 割り当 て、DHCP- Zeroconf	
企業とカメラ の LAN アップリ ンク	カメラの LAN アップリンク 専用経由	静的、DHCP 割り当 て、DHCP- Zeroconf	静的、DHCP 割り当 て、DHCP- Zeroconf	企業とカメラの LAN アップリ ンクは、別々のサブネットに配 置する必要があります。

初回のACC ES HD レコーダーの起動

ACC ES HD レコーダーは、ほこりや粒子、振動のない場所の、指定された動作温度範囲内に設置してください。指示に従わない場合、問題が生じても保証の対象になりません。

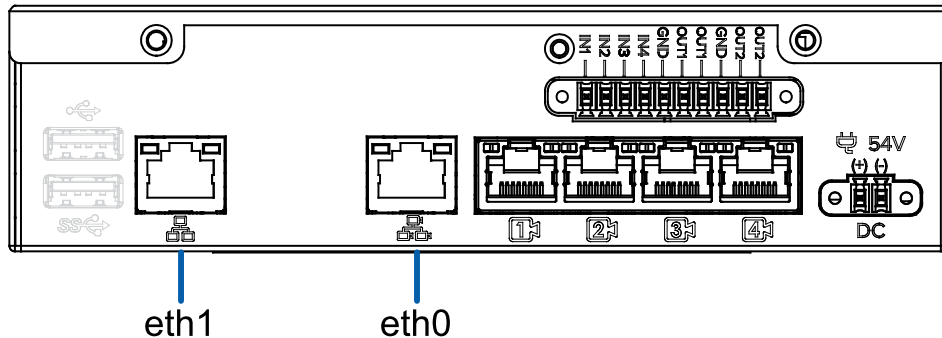
デバイスをセキュリティネットワークに接続する前に、デバイスの初回構成を行う必要があります。

重要：静的IPが必要な場合は、デバイスのIPアドレスを手動で構成するためにラップトップコンピューターが必要です。ラップトップにIP アドレス 169.254.100.99 または 169.254.100.100 が割り当てられておらず、IP サブネットマスクが 255.255.0.0 であることを確認します。

1. デバイ스에電源を接続し、起動するまで待ちます。初めて電源を入れたときは、起動に数分かかる場合があります。

アプライアンスのLED インジケーターで示されるステータスが正しいことを確認します。詳細については「LED インジケーター」（22ページ）参照してください。

2. 静的IPアドレスを持つデバイスを設定している場合、Ethernetケーブルを使って、構成しているラップトップのDHCP対応ポートを直接カメラネットワーク (eth0) ポートに接続します。それ以外の場合は、企業ネットワーク (eth1) ポートを使用して、デバイスを企業ネットワークに接続します。



3. 接続されているラップトップまたはネットワークワークステーションで、アプライアンスを検出します。Windowsコンピュータではエクスプローラーを、MacintoshコンピュータではFinder®を使用します。

「VMA-RPO-4Px< シリアル番号 >」というラベルの付いたネットワークデバイスを探しています。アプライアンスを見つけることができない場合は「トラブルシューティング」（33ページ）を参照してください。

4. クリックして、対応する Web ブラウザでデバイスを開きます。サポートされている Web ブラウザの

リストについては、「システム要件」(3ページ)をご覧ください。

重要: ACC ES HD レコーダーは、Webブラウザで接続警告を発する自己署名証明書で構成されています。

5. ブラウザで表示されたすべての接続メッセージをクリックしてください。ブラウザによっては2つの警告メッセージが若干異なります。ブラウザが…
 - Chromeの場合—最初の画面で**Advanced (高度)** をクリックして、2番目の画面で**Proceed to <IP address> (unsafe) (<IPアドレス> (危険) に進む)** をクリックします。
 - Firefoxの場合—最初の画面で**Advanced (高度)** をクリックして、2番目の画面で**Add Exception (例外を追加)** をクリックし、**Permanently store this exception (この例外を永久保存)** にチェックを入れて**Confirm Security Exception (セキュリティの例外を確認)** をクリックします。
6. デバイスが自己署名のWeb 証明書を使用しているため、Web UIとデバイス間の接続が信頼できないことを通知するセキュリティ警告がブラウザーに表示されます。これは想定内であり、警告を無視して安全にACC ES管理者Web UIに進むことができます。

デバイスに含まれる証明書によって提供されるセキュリティのレベルは、内部サーバーに公開キー基盤 (PKI) を展開しない組織にとって十分なものである必要があります。

重要: 独自のPKIを展開している組織の場合、デバイスをインストールして電源を入れた後、デバイスの証明書をACC ES管理者Web UIから管理できます。デフォルトの自己署名済みWeb 証明書を置き換えることができ、デバイスに提供されていない認証局 (CA) からの署名付き証明書を追加でき、デバイスに提供されているGoogle Mailなどのパブリックサーバー用のCAからの署名付き証明書を無効にできます。詳細については、「[「証明書の管理」\(25ページ\)](#)」を参照してください。

7. Web インターフェイスで指示が表示されたら、管理者ユーザー名の新しいパスワードを入力します。
強度メーターはパスワードの複雑さを測定します。赤は単純すぎ、黄は合理的に複雑、緑は複雑です。複雑さは、パスワードの安全性ではなく、パスワードを検出することの難しさを測定します。複雑なパスワードをお勧めします。
ページが更新され、ログインするよう求めるメッセージが表示されます。
8. ユーザー名に「administrator」と入力し、新しいパスワードを入力します。
Web インターフェイスのダッシュボードパネルが表示されます。

9. Web インターフェイスの言語、ユーザーフレンドリーなホスト名とタイムゾーンを設定します。ナビゲーションサイドバーで、**デバイス** をクリックして、デバイスパネルを開きます。
で
 - a. 一般ドロップダウンリストから言語を選択します。
 - b. ホスト名 ペインで、オプションとしてアプライアンスのシリアル番号をアプライアンスの記述ホスト名に入れ替えることができます。
 - c. 時刻 ペインで、タイムゾーンを指定し、NTPドロップダウンとサーバーリストでタイムソースを特定します。

詳細については、「デバイスの再起動とデバイス設定の管理」（12ページ）を参照してください。

10. アプライアンスがネットワークからIPアドレスを取得する方法を選択します。**ネットワーク** をクリックして、絞りを開きます。ネットワーク 使用されている各ネットワークポートのために、自動を選択するか、手動で設定を入力します。

詳細については、「「デバイスをユーザーとカメラに接続する」（15ページ）」を参照してください。

11. ラップトップを使用してデバイスを構成した場合：
 - a. デバイスから企業ネットワークにイーサネットケーブルを接続します。
 - b. 構成中のノートパソコンをカメラネットワークポートから外します。
12. PoE スイッチ コンポーネントにカメラを接続します。

Webインターフェイスの詳細については、「レコーダーの設定」（8ページ）を参照してください。

これで、ACCClient ソフトウェアをインストールし、ACC ES HD レコーダー を ACC サイトに接続する準備ができました。これで AvigilonControl Center Client ソフトウェアを通して、毎日の業務に使用するデバイスとカメラを構成することができるようになりました。詳細については、「ACC ソフトウェアと ACS への接続」（20ページ）」を参照してください。

レコーダーの設定

ACCESHDRレコーダーは、ネットワーク上の任意のブラウザからアクセスできるACCES管理者Webユーザーインターフェイス（ACCES管理者WebUI）を通じて設定することができます。ACCES管理者WebUIを使用すると、レコーダサーバー設定の設定、サーバーによる時間の記録方法などを設定できるほか、サーバーをリモートから再起動させたり、アップグレードしたりすることができます。ACCをクリックしてソフトウェアをダウンロードし、使用中のコンピュータにインストールして、ACCES管理者WebUIにアクセスします。

レコーダーを構成した後、レコーダーのシステム設定のバックアップを開始します。これらの設定には、ACCのパスワード、およびカメラ接続の設定が含まれます。サイトおよびサーバー構成のバックアップの詳細についてはAvigilonACCClientユーザーガイドを参照してください。

このセクション全体を通して、デバイスという用語はレコーダーと同じ意味で使用されます。

ACC ES管理者Web UIの起動

デバイスにネットワークアクセスできるネットワークワークステーションからACC ES管理者Web UIにアクセスできます。

デバイスのACC ES管理者Web UIに初めてアクセスするときは、次のいずれかの方法を使用します：

• デバイスの発見

1. ファイルエクスプローラー (Windows) またはFinder (Macintosh) で [ネットワーク] タブを開き、デバイスを探します。

「VMA-RPO-4Px<シリアル番号>」というラベルの付いたネットワークデバイスを探しています。

2. 右クリックして**デバイスのWebページを表示**を選択し、デフォルトのWebブラウザでデバイスのサインインページを開きます。

• IP アドレスまたはホスト名の使用

1. デバイスへのネットワークアクセスを備えたネットワークワークステーションからWebブラウザを開きます。
2. WebブラウザにIPアドレスまたはホスト名を入力して、デバイスサインインページを開きます：

`https://<デバイスIPアドレス>|<デバイスホスト名>/`

例えば： <https://169.254.100.100/> または https://my_AvigilonDevice/、ここでは my_AvigilonDevice/ がデバイスパネルで設定されたホスト名です。

メモ： インストールプロセス時に設定したIPアドレスまたはホスト名を思い出せない場合、その情報はサーバーの[セットアップ]タブにあるACCクライアントソフトウェアに記載されています。

ヒント： デバイスのサインイン Web ページの URL をブックマークします。

ACC ES管理者Web UIへのログインとログアウト：

1. ログインするには、ACC ES管理者Web UIのユーザー名とパスワードを入力します。

ユーザー名は常に「administrator」になります。最初にデバイスにログインしたときに設定したパスワードを使用します。詳細については、「初回のACC ES HD レコーダーの起動」（5ページ）を参照してください。

ACC ES管理者Web UI起動ページは、Webブラウザに表示されます。

2. ACC ES管理者Web UIからログアウトするには、最上部のバナーの右側にあるログアウトアイコンをクリックします。

ACC ES管理者Web UI起動ページのサイドナビゲーションバーで**ダッシュボード**が選択され、ダッシュボードステータスパネルが表示されます：

- **ACC サーバー** — ACCサーバーソフトウェアが動作しているときに**実行中**が表示され、それ以外の場合は**停止**が表示されます。パネルには、デバイスに関する技術情報（サイト名、サーバー名、サーバーID、サーバーのバージョン、ソフトウェアのバージョン、使用可能なカメラチャネルの数、および許可されているACCクライアントインスタンスの最大数）が表示されます。
- **システム** — デバイスが完全に動作可能なときに**準備完了**が表示され、そしてデバイスが再起動されたときに**再起動中**それから**初期化中**が表示されます。パネルには、デバイスに関する技術情報（製品名、部品番号、シリアル番号、およびファームウェアのバージョン）が表示されます。

ダッシュボードのナビゲーションバーのサービスおよびシステムのメニューオプションを使用して、他のすべてのWeb インターフェイスパネルにアクセスします。

- ・ **サービス** – 左サイドバーで **ACC** を展開して、次に移動します：
 - ・ デバイスでACCサーバーを制御するための**サーバー**ページ。「ACCサービスとストレージの管理」(11ページ)を参照してください
 - ・ ACCサーバーサービスログを表示する**ログ**ページ。参照してください「サポートのためのサービスログの提供」(12ページ)。
- ・ **システム** – デバイスを設定し、そのステータスを表示するための5つのオプションにアクセスします：
 - ・ **デバイス**。参照：
 - ・ 「デバイスの再起動とデバイス設定の管理」(12ページ)
 - ・ 「ファームウェアのアップグレード」(29ページ)
 - ・ 「証明書の管理」(25ページ)
 - ・ **ストレージ**。「ストレージドライブの状態の監視」(14ページ)を参照してください。
 - ・ **ネットワーク**。「デバイスをユーザーとカメラに接続する」(15ページ)を参照してください。
 - ・ **ログ**。「サポートのためのデバイスログの提供」(17ページ)を参照

PoEポートのステータスの表示

「PoE」パネルでは、各ポートのステータスが [ステータス] 列に表示されます。次の状態があります。

緑 一定 PoE デバイスがポートに接続され、正常に動作しています。

色 出力

高出 PoE +がオンになっています。
力

灰 切断 ポートに接続されているデバイスがありません。

色

出力 PoEポートの電源は、ACC ES管理者Web UIのPoEページからスイッチオフされます
なし

黄 過負 PoE デバイスはポートに接続されていますが、電力を受け取っていません。このステータス
色 荷 は、通常、一つのポートが過電流の場合や、デバイスが配分以上の電力を要求している場合などに生じます。

低出 デバイスはポートから低電流を得ています。
力

赤 エ デバイスがエラー状態です。
ラー

ヒント: カメラを外した後で再度デバイスに接続した場合、このページを更新して最新のステータスを確認し、値を配分しなければならないことがあります。

ACCサービスとストレージの管理

サーバーパネルでは：

- 一般 ペイン：

タスク	操作
デバイスをシャットダウンする前に、すべてのサービスをシャットダウンします。	停止 をクリックします。
サービスがシャットダウンされた後ですべてのサービスを起動します。	開始 をクリックします。
ストレージドライブをフォーマットします。	再初期化 をクリックしてすべての設定と記録映像データを削除します。

- ネットワークストレージ管理 ペインを使用します。

ユーザーが ACC クライアントソフトウェアを使用してこのデバイスからのビデオをアーカイブできるようにするには：

- 有効** をクリックします。
- [Protocol(プロトコル)] ドロップ ダウン リストで、次のいずれかを選択します。
 - CIFS(CIFS)** – 共通のインターネット ファイル システム。ネットワーク パスは一般的に次の形式を取ります：//<ホスト名または IP> / <パス>
 - NFS(NFS)** – ネットワーク ファイル システム。ネットワーク パスは一般的に次の形式を取ります：//<ホスト名または IP> : <パス>
- [**ネットワークパス**] フィールドに、希望のビデオアーカイブロケーションへのパスを入力します。
- ネットワークロケーションに認証が必要な場合、[**ユーザー名**] と [**パスワード**] フィールドに認証資格情報を入力します。
- [**適用**] をクリックします。

- サービスとRTPポートのペイン

デバイスとの通信に使用するUDPポートとTCPポートを変更するには：

- サービスポートペインで、HTTP、HTTPSおよびUDPポートに使用する**基本値**を入力し、**適用**をクリックします。ポートのリストが更新されます。
- RTPポートペインで、UDPポートに使用される**基本値**を入力して**適用**をクリックします。RTPで利用可能なポートの範囲が更新されます。

重要：これらの変更は、システムの再起動後にのみ有効になります。プロンプトが表示されたら、システムを再起動します。

サポートのためのサービスログの提供

ログページを使用してサービスログを表示します。問題解決に役立てるために、通常 Avigilon テクニカルサポートからログを求められます。

デフォルトでは、ログからの 100 件の警告メッセージがページに表示されます。

通常、Avigilonテクニカルサポートは、このパネルのログにアクセスしてフィルタリングし、必要なログを分離するのに役立ちます。次に、ログをコピーしてテキストファイルに貼り付け、保存して、Avigilonテクニカルサポートに送信します。

ログをフィルタリングして、必要な上布を表示することができます。

1. ドロップダウンリストで、必要になるアプリケーション ログの種類を選択します。オプション：
 - **例外ログ**
 - **FCP ログ**
 - **サーバー ログ**
 - **WebEndpoint ログ**
2. **[最大ログ]** ドロップダウン リストから、毎回表示させるログ メッセージの数を選択します。
3. **フィルター** フィールドにテキストを入力して、ログリストにフィルターを適用します。
4. 更新ログを表示するには**Sync (同期)** ボタンをクリックします。

デバイスの再起動とデバイス設定の管理

デバイスパネルでは：

- **一般**ペインを使用して：
 - ACC ES管理者Web UIから、デバイスを
 - **再起動**します。デバイスがACC ES管理者Web UI起動ページから再起動するとき、デバイスの進行状況を監視することができます（詳細については、「ACC ES管理者Web UIの起動」（8ページ）を参照してください）。
 - ドロップダウンリストから、ACC ES管理者Web UIの **言語**を選択します。
- **ホスト名**ペインを使用して新しい**ホスト名**を入力します。**適用**をクリックして変更を行います。
デフォルトのホスト名はサーバー名と同じです。サーバー名は、<モデル>-<シリアル番号>フォームにあります
- **パスワード**ペインを使用して管理者パスワードを変更します。

メモ：ACC ES管理者Web UI でデフォルトのユーザー名*administrator*ユーザー名を変更することはできません。変更できるのはパスワードのみです。

1. パスワードを変更するには、現在のパスワードを[**古いパスワード**]フィールドに入力して、身元を確認します。
2. [**新しいパスワード**]フィールドに新しいパスワードを入力します。
3. [**パスワードの確認**]フィールドに新しいパスワードを再入力します。

注意—パスワードを忘れた場合、録画されたビデオと設定データは失われます。管理者パスワードをリセットするには、デバイスを工場出荷時のデフォルト設定にリセットする必要があります。こうすると、ハードドライブがフォーマットされて、構成データと録画ビデオも削除されます。工場出荷時の設定への復元の実行方法については、「工場出荷時の設定への復元」（31ページ）を参照してください。

- **時刻**ペインを使用してデバイスが時刻を保持する方法をカスタマイズします：
 - ドロップダウンリストから**タイムゾーン**を選択します。あなたがここで設定したタイムゾーンはACCクライアントソフトウェアで定義された録画スケジュールで使用されています。
 - NTPフィールドで、ネットワークタイムプロトコル（NTP）サーバーにより同期された時間を維持する（推奨）かどうかを選択します。
- 選択：
- **DHCP**—ネットワークで自動的に既存のNTPサーバーを使用する。
 - **手動**—このオプションを選択し、続いてNTPサーバーのアドレスを[サーバー]リストに入力します。リスト内のアドレスを追加および削除し、それらを並べ替えるコントロー

ルがアクティブになります。

- オフ NTPサーバーを使用していない場合。

メモ : NTPサーバーのデフォルトのセットは、常にサーバーリストにあります。デフォルトのリストは再配置または削除できません。

- 0.pool.ntp.org
- 1.pool.ntp.org
- 2.pool.ntp.org
- 3.pool.ntp.org





適用をクリックして、時間設定を保存します。

- **ファームウェアのアップグレード**ペインを使用して、お使いのデバイスのファームウェアの最新バージョンをインストールしたり、破損した場合、ファームウェアを再インストールしたりします。詳細については、「「ファームウェアのアップグレード」 (29ページ) 」を参照してください。
- ACC ES管理者Web UIとデバイスが使用する証明書を管理する**証明書**ペイン。詳細については、「証明書の管理」 (25ページ) を参照してください。

ストレージドライブの状態の監視

ストレージパネルには、ACC ES 4および8ポートアプライアンス（または古い4ポートACC ESアプライアンスのドライブ）のデバイスのストレージ容量と、ストレージドライブのステータスを表示できます。

ストレージパネルを開くには、ナビゲーションバーの**ストレージ**をクリックします。ストレージパネルのペインで次のどのアクションも実行できます：

タスク	操作
ストレージドライブの容量とステータスを表示します。	デバイスが次の場合： <ul style="list-style-type: none">• 正しく動作し、準備完了と  が表示されます。• 正しく動作せず、エラーと  が表示されます。
ドライブの詳細を表示します。	<ol style="list-style-type: none">1. ストレージの詳細ペインを開くには、ペインの右上にある  をクリックします。2. そのモデルとシリアル番号など、ドライブに関する詳細を表示するには、  をクリックします。

デバイスをユーザーとカメラに接続する

ネットワークパネルでは、デバイスのネットワーク接続を変更できます。2つのネットワーク接続をサポートしています。1つは企業ネットワークを対象としたもので、もう1つはカメラネットワークを対象としたものです。

メモ： 企業ネットワークとカメラネットワークを異なるIPサブネット上に配置する必要があります。

企業ネットワークは、通常、ユーザーにデバイスへのアクセスを提供するネットワークです。ACCClient ソフトウェア経由でビデオをモニタするユーザーは、このネットワーク経由でデバイスに接続します。

重要： アプライアンスを新しい ACC サイトとして追加するか、またはアプライアンスを既存の ACC サイトにマージする前に、IP アドレスを設定します。ACC サイト内の他のサーバーと同じ IP サブネットに配置することを強くお勧めします。

カメラネットワークは、通常カメラのみが含まれる閉じられたネットワークです。これにより、録画に対する干渉の量が少なくなります。

ONVIF デバイスをカメラネットワークに接続する際、アプライアンスが ACC 7.x 以降を実行している場合は、アプライアンスをその時刻/NTP サーバーとして使用するよう構成します。

ネットワーク接続に関する詳細は、「サポート対象のネットワーク構成」(4ページ)を参照してください。

ネットワークパネルの各ペインで次のどのアクションでも実行できます。

タスク

操作

デバイスがネットワークごとに IP アドレスを取得する方法を設定する

自動をオンにすると、接続されているネットワークを自動的に検出し（デフォルト設定）、手動で接続を指定するにはオフにします。手動で接続設定を入力する場合は、以下のフィールドに適切な値を入力します。

ネットワークパネルの各ペインで、接続されたネットワークを自動的に検出するには**自動IP**をオンに切り替え（デフォルト設定）、手動で接続を指定するにはオフにします。手動で接続設定を入力する場合は、以下のフィールドに適切な値を入力します。

• IP アドレス

タスク

操作

- サブネット マスク
- デフォルト ゲートウェイ

[適用] をクリックして、変更を保存します。

デバイスが DNS サーバーから名前付きアドレスを取得する方法を設定します。


自動 DNSをオンにすると、接続されているDNSサーバーが自動的に検出され（デフォルト設定）、手動でDNSサーバーを指定するにはオフにします。**自動 DNS**を切り替えると、リスト内のアドレスを追加および削除し、それらを並べ替えるコントロールがアクティブになります。

PoE 電源予算の割り当て

PoEパネルを使って、接続されているデバイスにどれだけの電力が供給可能であり、また使用されたかを確認します。すべてのポートのデフォルト設定は自動です。この設定は、ポートに接続されたデバイスが必要とする電力量を自動的に検出し、配分を設定します。各ポートについて、この設定を手動で調整するか、電源出力を完全にオフにすることができます。手動でポートの電力出力を調整する場合は、PoE 電力配分を計算する場合は、「PoE 電源への電力配分」（24ページ）を参照してください。

ヒント：高電力 PoE を必要とするカメラにミッドスパン PoE パワーインジェクタを使用している場合は、その PoE ポートをオフに設定する必要があります。

PoEパネルを開くには、次のいずれかを実行します。

- ACC ES管理者Web UI起動ページのPoEステータスパネルにをクリックしてください。
- ダッシュボードのナビゲーションバーから**PoE**をクリックします。

タスク

操作

接続されているデバイスにどれだけの電力が供給可能であり、また使用されたているかを確認できます。

パネルの上部にある2つのバーを見てください。

- **電源容量**バーは、PoEポートに接続されているすべてのデバイスに割り当てられている総電力量を示します。
- **消費量**バーは、接続されているすべてのデバイスで現在使用されている実際の電力量を示します。

各PoEポートが使用する電力を調整します。

に**電力**バーを使用して、PoE電力配分を設定します。

ヒント: また、電力バーを使用して、カメラをリモートで再起動することもできます。電力設定をオフに設定したら、カメラの電源が切れるのを待ち、続いて電力設定を**自動**または**手動**に変更します。

ヒント: PoEとPoE + (802.3at) の両方の動作モードに対応するデバイスは、手動の15W配分を使用して非PoE +モード (802.3af) に強制することができます。

- **オフ**をクリックしてポートへの電力出力を無効にします。ポートへの電力が無効になると、ポートは電力を出力しなくなりますが、任意のデバイスの標準ネットワーク接続の機能を果たすことができます。
- **自動**をクリックして、接続されたデバイスの動作モードに応じてデバイスに自動的に電力が出力されるようにします。
- **手動**をクリックして、ワット単位で電力配分値を入力します。ケーブルの電力損失の可能性も配分に含めるようにしてください。

設定は **[適用]** をクリックするまで実装されません。

[適用] をクリックしたら、次のメッセージが表示されたときにシステムが再起動することを許可します。

変更内容を適用すると、PoE受電デバイスに対して電源サイクルが実行される可能性があります。

ACC ES管理者Web UIによって画面が自動更新され、新しい電力設定の適用が完了すると、更新された設定が表示されます。

サポートのためのデバイスログの提供

システム ログパネルを使用してデバイスのログを表示します。問題解決に役立てるために、通常 Avigilon テクニカルサポートからログを求められます。

デフォルトでは、ログからの 100 件の警告メッセージがページに表示されます。

通常、Avigilonテクニカルサポートは、このパネルのログにアクセスしてフィルタリングし、必要なログを分離するのに役立ちます。次に、ログをコピーしてテキストファイルに貼り付け、保存して、Avigilonテクニカルサポートに送信します。

ログをフィルタリングして、必要な上布を表示することができます。

1. ドロップダウンリストで、必要になるアプリケーション ログの種類を選択します。オプション：
 - システム ログ
 - ブート ログ
 - Web サーバー ログ
2. [最大ログ] ドロップダウン リストから、毎回表示させるログ メッセージの数を選択します。
3. フィルターフィールドにテキストを入力して、ログリストにフィルターを適用します。
4. 更新ログを表示するには**Sync (同期)** ボタンをクリックします。

ACC Client のインストールと起動

セキュリティネットワークに最初のAvigilonアプライアンスをインストールする場合、ネットワークワークステーションまたは Web インターフェイスへのアクセスに使用しているコンピュータにACC Client ソフトウェアをインストールできます。それ以外の場合は、ネットワークワークステーションでACC Client ソフトウェアを使用して、アプライアンスをセキュリティネットワークの新しいサイトとして追加するか、または既存サイトにマージします。

重要：アプライアンスを新しい ACC サイトとして追加するか、またはアプライアンスを既存の ACC サイトにマージする前に、IP アドレスを設定します。ACC サイト内の他のサーバーと同じ IP サブネットに配置することを強くお勧めします。


インターネットへのネットワークアクセスが可能なネットワークワークステーションにACC Client ソフトウェアの最新バージョンをインストールできます：

1. インターネットへのネットワークアクセスを備えたネットワークワークステーションからWebブラウザを開きます。
2. ACCClient ソフトウェアを、Avigilon Web サイトavigilon.com/support/softwareからダウンロードします。ACC Client ソフトウェアの最新バージョンのインストールソフトウェアをクリックスルーします。

メモ：ソフトウェアをダウンロードするWebサイトに初めてアクセスすると、登録を求められます。必要な情報をすべて入力し、**登録の完了**をクリックします。登録は自動的に承諾され、Webサイトに進みます。

3. ACCClient ソフトウェアを、デバイスへのネットワークアクセスを備えたワークステーションにインストールします。

ACC クライアントソフトウェアを開く手順：

- デスクトップショートカットアイコン  をダブルクリックします。
- スタートメニューから、**[すべてのプログラム]** または **[すべてのアプリケーション]** を選択し、**Avigilon > Avigilon Control Center クライアント** の順にクリックします。

ACC クライアントソフトウェアを閉じる手順：

1. 右上隅で、**×** をクリックします。
2. **[はい]** をクリックします。

ACC ソフトウェアと ACS への接続

アプライアンスを展開したら、ACC ソフトウェアを活性化し、Avigilon クラウドサービス (ACS) に接続する必要があります。

ACC ソフトウェアのアクティブ化と構成

- [ACC™ システム初期設定およびワークフロー ガイド](#)
- [ACC 7ヘルプセンター](#)

これらのガイドの印刷用バージョンは次のAvigilonウェブサイトでご覧いただけます：avigilon.com/support/software/。

Avigilonクラウド サービスへの接続

それにより、ACC ソフトウェアをアクティブ化した後、ACC サイトを無料でクラウドに接続し、分散システム全体に集中型アクセスを提供する機能を利用できます。

サイトをAvigilon クラウド サービスに接続するには、help.avigilon.com/cloud を参照してください。

クラウド サービスに関する情報については、[Avigilon クラウド サービス サポート](#)を参照してください。

ACC クライアントソフトウェアのスタートアップとシャットダウン

ACC クライアントソフトウェアを開く手順：

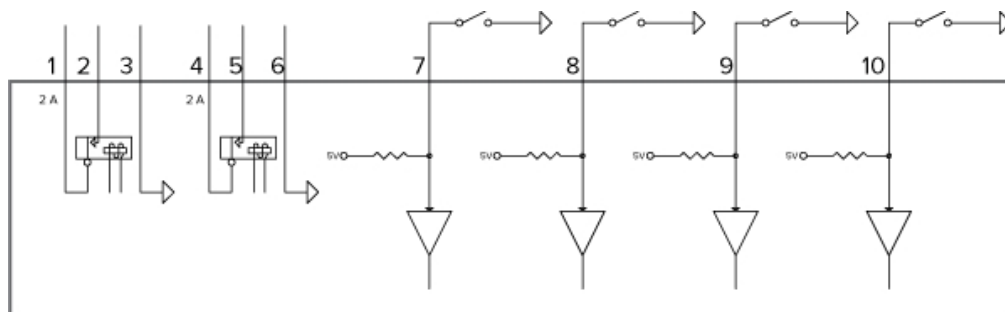
- デスクトップショートカットアイコン  をダブルクリックします。
- スタートメニューから、**[すべてのプログラム]** または **[すべてのアプリケーション]** を選択し、**Avigilon > Avigilon Control Center クライアント**の順にクリックします。

ACC クライアントソフトウェアを閉じる手順：

1. 右上隅で、**×** をクリックします。
2. **[はい]** をクリックします。

外部デバイスへの接続

外部デバイスは、I/O端末経由でレコーダーに接続されます。I/O端子のピン配列を次の図に示します。



1. 出力 2 (リレー出力) — Form-A ドライ接点出力。アクティブなときは、端子が接続されています。非アクティブな場合、端子はオープン状態です。

最大負荷は 30 V、2 A または 200 V、250 mA です。

2. 出力 2

3. アース (GND)

4. 出力 1 (リレー出力) — Form-A ドライ接点出力。アクティブなときは、端子が接続されています。非アクティブな場合、端子はオープン状態です。

最大負荷は 30 V、2 A または 200 V、250 mA です。

5. 出力 1

6. GND (アース)

7. 入力 4 (アラーム入力) — アクティブロー入力。アクティブ化するには、入力をアースピン (GND) に接続します。非アクティブ化するには、切断された状態のままにするか、3~15Vを印加します。

8. 入力 3

9. 入力 2

10. 入力 1

LED インジケータ

以下の一覧に、ACC ES HD レコーダーのLEDの意味を説明します。

フロントパネルのLED

アイコン	LEDの状態	説明
	緑色	デバイスの電源が入り、稼働中です。
	オレンジ色	デバイスを再起動中です。
	オレンジ - 点滅	工場出荷時設定への復元ボタンが押されました。
	緑色	ハードディスクドライブが接続されています。
	赤	ハードディスクドライブの接続にエラーがあります。
	緑色	カメラはネットワーク接続とパワーオーバーイーサネット (PoE) の電源のスイッチを使用しています。
	オレンジ色	カメラはネットワーク接続のみのスイッチを使用しています。
	オレンジ - ゆっくり点滅	システムオーバーパワーバジェット警告詳細については、Webインターフェイスの[PoE]パネルを確認してください。 <ul style="list-style-type: none">一方のポート全ポート
		システムの使用電力がPoE電力バジェットを超えているためポートがオフになっています。
		システムがPoE電力バジェットを超えています。 詳細については、「[PoE 電源予算の割り当て] (16ページ)」および「[PoEポートのステータスの表示] (10ページ)」を参照してください。
	緑色 - オレンジ色が交互に点灯	エラーのためにポートがオフになっています。

アイコン	LEDの状態	説明
	オレンジ色	GigE ネットワークリンクが存在します。
	緑色	10/100 ネットワークリンクが存在します。
	オレンジ色	スイッチコンポーネントが、PoE 出力機能の上限に達しました。

バックパネルのLED

アイコン	LEDの状態	説明
	緑色	ネットワークアクティビティが存在します。
	オレンジ色	GigE 速度でオンになっています。10/100 速度でオフ。
	緑色	ネットワークアクティビティが存在します。
	オレンジ色	100M 速度でオン。10M 速度でオフ。

PoE 電源への電力配分

4ポート式デバイス上のPoE スイッチ コンポーネントでは、合計 64W の電力を接続されているデバイスに出力することができ、8ポート式デバイス上のものであれば、合計128Wの電力を出力できます。いずれのPoE ポートも16 Wを標準PoEデバイスに、また30 WをPoE+デバイスに出力することができます。これは通常、4ポート式デバイスが標準 PoE デバイスを4つまで、または PoE+ デバイスを2つまでサポートでき、8ポート式デバイスが標準 PoE デバイスを8つまたはPoE+ デバイスを4つまでサポートできることを意味します。

上級ユーザーは、ポートごとに PoE の電力配分を手動で調整して、必要とされるカメラに常時対応できるようにすることができます。

各ポートの PoE 配分を手動調整する場合は、ケーブルにおける電力損失の可能性も計算に入れる必要があることにご注意ください。ケーブルにおける電力損失の量がわかっている場合を除き、次の推定値を使用してください。

- デバイスの使用電力が16 W 以下の場合 – 2.5 W の電力損失を想定します。
- デバイスの使用電力が 16 W 超の場合 – 4.5 W の電力損失を想定します。

ポートごとの推奨電力配分を計算するには、次の方程式を使用してください。

$$\text{電力配分} = \text{<カメラの消費電力>} + \text{<想定されるケーブルの電力損失>}$$

例：次の 4 台のカメラを4ポート式デバイスに接続する場合：

$$\text{HD ドーム型カメラ 2 台} \quad (9 \text{ W} + 2.5 \text{ W}) \times 2 = 23 \text{ W}$$

$$\text{HD PTZ カメラ 1 台} \quad 25.5 \text{ W} + 4.5 \text{ W} = 30 \text{ W}$$

$$\text{HD マイクロドーム 1 台} \quad 4 \text{ W} + 2.5 \text{ W} = 6.5 \text{ W}$$

$$\text{合計} = 59.5 \text{ W}$$

4 台のカメラの合計消費電力は、PoE スイッチコンポーネントの制限値の範囲内です。

メモ： PoE ポートに必要な電力の計算を誤った場合、合計出力が 64 W を超えると接続されているカメラがシャットダウンすることがあります。

証明書の管理

信頼できる証明書は、デバイスが接続に必要な他のサーバーとクライアントを認証し、それらの接続を保護するためにデバイスによって使用されます。Avigilon自己署名済みのWeb 証明書を提供して、ACC ES管理者Web UIとWebEndpointサービス、および信頼されたCAからの一連のシステムレベルの署名済み証明書への接続をセキュリティ保護し、必要なあらゆるサーバーへの安全な接続を保証します。オプションで、独自の証明書とCAを提供できます。

デバイスに含まれる証明書によって提供されるセキュリティのレベルは、内部サーバーに公開キー基盤 (PKI) を展開しない組織にとって十分なものである必要があります。

アプライアンスの証明書管理機能は、ACC ES管理者Web UIと ACC WebEndpoint 製品で使用されるアプライアンスの Web 証明書のみを制御します。ACCサーバー内では、この機能によって構成された認証局は、ACC電子メールおよび中央ステーション監視機能によって使用される安全な電子メールサーバーを検証するためにのみ使用されます。ACCサーバーからACCサーバーへ、およびACCサーバーからACCクライアントへの接続の制御または検証には、アプライアンスの証明書管理機能を使用しません。

たとえば、組織がGoogle Mailなどのパブリックメールサーバーを使用している場合、メール通知がトリガーされると、ACCはGoogleメールサーバーにアクセスし、Googleメールサーバーを識別する証明書を受け取ります。ACCソフトウェアは、Google Mail証明書に署名したCAが既知の信頼できるCAのリストからのものであり、接続が保護されていることを確認して、証明書を検証します。

メモ： デバイスに同梱された署名済み証明書は、Mozillaのブラウザに同梱されたものと同じであり、[The Debian Project](#)から公的に入手可能です。証明書により、SSLベースのアプリケーションがSSL接続の信頼性をチェックできます。Avigilonは、証明書がこのアプライアンスに含まれている証明機関が信頼性やRFC 3647準拠のための監査を受けているかどうかを確認することも否定することもできません。それらを評価する完全な責任は、ローカルシステム管理者にあります。

自社のPKIを展開する組織は、ACC ES管理者Web UIの [証明書] ペインを使用して、デバイス上の証明書を管理できます。

たとえば、次のことができます：

- デフォルトの自己署名済みWeb 証明書を自分の組織の証明書に置き換えます。
- 組織内で使用されている内部CAなどのCAをデバイスに追加します。
- システムレベルのCA証明書を無効（および有効）にします。

Web 証明書の交換

デバイスのWeb 証明書を [証明書] ペインの [Web 証明書] タブで管理します。ACC ES管理者Web UIとWebEndpointサービスは、この証明書を使用して、接続しているデバイスに対して自身を認証します。いつでもアクティブにできるWeb 証明書は1つだけです。

デフォルトのWeb 証明書をカスタム証明書に置き換えることができます。

重要： デバイスを出荷時の設定にリセットする（出荷時リセットとも呼ばれる）場合、カスタム証明書をリロードする必要があります。

新しいWeb 証明書の取得は、3ステップのプロセスです：

1. 組織で使用されている証明書発行者に証明書署名要求 (CSR) を送信すると、発行者から新しい証明書ファイルと秘密キーファイルが返されます（通常は電子メール）。彼らがACC ES管理者Web UIからCSRを受け入れない場合、[Web 証明書] タブ、または証明書発行者の好適な方法を使用してからCSRを生成できます：
 - a. Web UIを開いて、ナビゲーションバーでデバイスをクリックし、証明書ペインまでスクロールします。
 - b. [Web 証明書] タブで、証明書署名要求ボタンをクリックしてください。
 - c. 標準CSRフォームに、使用しているPKIによって定義された情報を入力し、生成をクリックします。
CSRファイルgenerated.csrは、ダウンロードフォルダに保存されます。
 - d. ファイルを組織の証明書発行者に送信します。

ヒント： 証明書発行者がCSRを受け入れない場合は、証明書発行者が推奨する方法を使用してCSRを生成します。

2. 証明書発行者からの新しい証明書を含む.crtファイルを受け取ったら、デバイスにアクセスできる場所に保存します。

3. 新しい証明書をデバイスにアップロードします :

- a. Web UI を開いて、ナビゲーションバーでデバイスをクリックし、証明書ペインまでスクロールします。
- b. [Web 証明書] タブで、アップロードをクリックします。
- c. [Web 証明書のアップロード] ダイアログで、証明書の名前を入力して、.crtファイルに移動するか、またはDrop '.crt' certificate (pem) file here or click to upload領域にドラッグ&ドロップします。
 - 証明書ファイルがACC ES管理者Web UIから生成された最新のCSRファイルで作成された場合、アップロードがアクティブ化されます。
 - それ以外の場合は、クリックして.keyファイルに移動するか、またはDrop '.key' private key (pem) file here or click to upload領域にドラッグアンドドロップします。アップロードがアクティブ化されます。

メモ : 証明書ファイル(.crt)が、証明書発行者の推奨する方法で生成されたCSRで作成された（またはデバイス上の最新のCSRファイルを使用して生成されなかった）場合は、この手順を繰り返して秘密鍵ファイルをアップロードします。

- d. [アップロード] をクリックします。

4. [Web 証明書] タブで、アップロードした証明書の名前をクリックして有効にします。これにより、以前の証明書も無効になります。

信頼できるCA証明書をアップロードする

証明書の[ユーザー認証局]タブから、組織の内部のサーバーに配備内部のCAから署名された証明書を管理します。

たとえば、独自のPKIを展開する組織の内部電子メールサーバーは、メールサーバーにアクセスしようとすると、既知の信頼できるCAのセットに含まれていないCAによって署名された証明書をACCソフトウェアに提供する場合があります。そのCAによって署名された証明書が[証明書] ペインの[ユーザー認証局] タブにアップロードされない限り、証明書を検証できません。

CAから署名済み証明書をアップロードする必要がある場合は、以下の手順を実行します :

1. ウェブUIを開き、ナビゲーションバーにデバイスをクリックし、[証明書]ペインまでスクロールします。
2. [ユーザー認証局] タブをクリックします。
3. [アップロード] をクリックします。

4. [ユーザー認証局のアップロード]ダイアログで、証明書の名前を入力し、クリックまたはドラッグアンドドロップしてファイルをアップロードします。一度にアップロードできるファイルは1つだけです。

ファームウェアのアップグレード

ACC ES管理者Web UIを使って、ファームウェアをアップグレードすることができます。

メモ： デバイスに接続されているACC Client からファームウェアをアップグレードすることもできます。ACCクライアントに付属のヘルプファイルにあるサイトのサーバーをアップグレードする手順を参照してください。

確実にレコーダーを最新のソフトウェアで動作させ、古いソフトウェアからアップグレードさせ、破損したファームウェアを交換するために、ファームウェアをアップグレードしてください。ファームウェアをアップグレードする際に、すべての現在の設定と録画されたすべてのビデオが保持されます。

破損したファームウェアをアップグレードするように選択すると、工場出荷時の設定に戻すことを回避するのに役立ちます。工場出荷時の設定に戻すと、構成されているすべての設定が失われ、記録済みのビデオがすべて削除されます。

ファームウェアをアップグレードまたは再インストールする前に、最新バージョンのファームウェア（.fp）ファイルを Avigilon Web サイト：partners.avigilon.com からダウンロードし、そして：

1. ACCES管理者Web UIを使用しているときにWebブラウザからインターネットにアクセスできる場合は、ダッシュボードから情報パネルに移動します。そして**ファームウェアのアップデート**をクリックします。

そうでない場合は、インターネットに接続されたワークステーションからpartner.avigilon.com に移動し、適切なACC ES(ACC ES)ファームウェアをダウンロードしてください。

2. ファイルをACC ES管理者Web UIにアクセスできる場所に保存します。

ACC ES管理者Web UIからファームウェアをアップグレードするには：

1. [デバイス] パネルに移動します。
2. 必要に応じ、スクロールしてファームウェアのアップグレードペインを表示します：
3. 次のいずれかの方法を使用します。

- ドラッグアンドドロップ

1. エクスプローラーを使用して、ダウンロードしたファームウェアファイルの場所に移動します。
2. エクスプローラー ウィンドウ内のファイルをクリックし、**'fp' ファイルをここにドロップするか、クリックしてアップロードします**エリア上にドラッグします。

- クリックしてアップロードします。
 1. **' .fp' ファイルをここにドロップするか、クリックしてアップロードします**エリアをクリックします。Windowsの開くダイアログボックスが表示されます。
 2. エクスプローラーを使用して、ダウンロードしたファームウェアファイルの場所に移動します。
 3. 開くダイアログボックス内のファイルをクリックし、**開く**をクリックします。
- 4. **OK** をクリックして続行を確認します。アップロードの進行状況インジケータが表示されます。ファイルがアップロードされ、確認されるまで待ちます。ファイルが確認されると、デバイスは再起動します。デバイスが再起動している間にWeb UI の通信が失われましたメッセージが表示されます。この手順には数分かかります。デバイスが再起動すると、ACC ES管理者Web UIへの接続がWebブラウザに復元されます。

進行中のファームウェアのアップロードするは、アップロードおよび確認段階でのみキャンセルできます。ファイルがアップロードされる前に、**アップロードのキャンセル**をクリックしてください。

メモ： アップロード段階またはアップグレードプロセス中にエラーが生じた場合や、ファームウェアが破損した場合は、ファイルを削除するように促されます。

リセット ボタンの使用

リセットボタンはレコーダーの正面にあります。システムステータス LED の左側にある、ラベルのない小さい○がこのボタンです。詳細については、「正面図」（2ページ）」を参照してください。

リセットボタンには2つの機能があります。

- システムの再起動 – レコーダーでシステムエラーが発生した場合、強制的に再起動させることができます。
- 工場出荷時の設定への復元 – ACC ソフトウェアが期待したとおりに機能しなくなった場合に、レコーダーを工場出荷時の設定にリセットすることができます。構成設定と収録されているデータはすべて削除されます。

メモ：リセットボタンを使用する場合、レコーダーに電源が投入されている必要があります。

システムの再起動

レコーダーでシステムエラーが生じてWebインターフェイスにアクセスできなくなった場合、物理的なレコーダーからシステムを再起動して問題の解決を試みることができます。

- 引き伸ばしたペーパークリップなどを使って、リセットボタンをそっと押し、離します。



注意 – 過剰な力をかけないでください。工具を奥に押し込めすぎると、レコーダーが損傷し、保証が無効になることがあります。

重要：リセットボタンを長押ししすぎないでください。長押ししすぎると工場出荷時の設定に復元されてしまいます。

工場出荷時の設定への復元


ACC サーバー ソフトウェアが期待したとおりに機能しなくなったり、管理者パスワードを思い出せなくなったりした場合に、レコーダーを工場出荷時の設定にリセットすることができます。

メモ：工場出荷時の設定に復元すると、インストールしたカスタム証明書を含め、すべての構成設定と記録映像が削除されます。工場出荷時のデフォルト設定が復元された後、機能上の問題が発生する前からの、最新のシステムバックアップを復元できます。カスタム証明書をリロードして、ACCサーバーソフトウェアを最新のリリースの更新が必要となる場合もあります。

1. 引き伸ばしたペーパークリップなどを使って、リセットボタンを軽く押し続けます。



注意 — 過剰な力をかけないでください。工具を奥に押し込めすぎると、レコーダーが損傷し、保証が無効になることがあります。

2.  LED がオレンジで点滅するようになるまで、ボタンを押すのをやめないでください。

トラブルシューティング

デバイスを検出できません

ハードウェアの設置中にエクスプローラー（Windowsの場合）またはFinder（Macintoshの場合）を使用してもデバイスを検出できない場合、しかもネットワークに接続されている場合は、次の手順を実行してください。

- `https://VMA-RPO-4P-<シリアル番号>`のURLを使用してWebブラウザからアプライアンスにアクセスします。
- アドレス解決プロトコル（ARP）を使用して、デバイスのIPアドレスを決定します：
 1. シリアル番号タグに記載されているMACアドレス（MAC）を見つけます。
 2. コマンドプロンプトウィンドウを開いて、以下のコマンドを入力します：

```
arp -a
```
 3. 応答をスクロールし、MACアドレスに対応するIPアドレスを探します。
- ACCクライアントソフトウェアからDHCPで割り当てられたIPアドレスを検出します。
 1. ACCClientソフトウェアをダウンロードして開き、構成ノートパソコンにインストールします。詳細については、「ACCClientのインストールと起動」（19ページ）を参照してください。
 2. 次の命名規則を使用するサイトにログインします: `VMA-PRO-4Px<シリアル番号>`。

メモ： Web インターフェイスアプリケーションのユーザー名とパスワードは、ACCサーバーの管理者ユーザー名とパスワードとは別です。

3. サーバーの[セットアップ]タブを表示します。
ウィンドウ最上部に、IP アドレスが表示されます。
4. Web ブラウザを開き、IP アドレスを次の形式で入力します：`https://<IP アドレス>`。
5. レコーダーをインストールする残りの手順を続けます。

ネットワーク構成

デフォルトでは、ACC ES HD レコーダー が DHCP を通じてネットワーク上の IP アドレスを取得します。静的 IP アドレスや特殊なネットワーク構成を使用するために ACC ES HD レコーダーを設定する必要がある場合、「デバイスをユーザーとカメラに接続する」(15ページ) で詳細を参照してください。

システム正常性のチェック

ACC Client ソフトウェアでサイトヘルス におけるシステムコンポーネントのヘルスを確認することができます。詳細については、ACC Client ユーザーガイドの[サイトヘルス](#)を参照してください。

詳細について

その他の製品マニュアルについては、Avigilon (avigilon.com) にアクセスしてください。

技術サポート

Avigilon技術サポートへのお問い合わせは、<http://avigilon.com/contact-us/> にアクセスしてください。

アップグレード

ソフトウェアおよびファームウェアのアップグレードは、利用可能になるとダウンロードして入手できます。可能なアップグレードについては、avigilon.com/support-and-downloadsにてご確認ください。

フィードバック

私達はお客様からのフィードバックを大切にしています。当社の製品およびサービスに関するコメントは、feedback@avigilon.com に送信してください。

制限付き保証および技術サポート

この製品のAvigilon 保証条件は、[avigilon.com/warranty](https://www.avigilon.com/warranty) に規定されています。

保証サービスと技術サポートは、Avigilon 技術サポート: [avigilon.com/contact/](https://www.avigilon.com/contact/) に連絡して受けることができます。