証明書
SANtricity 11.6

NetApp
February 12, 2024

目次

証明書

概念

証明書の仕組み

証明書は、Webサイトやサーバなどのオンラインエンティティを識別するデジタルファイルで、インターネット上のセキュアな通信を実現します。

証明書を使用すると、指定されたサーバとクライアント間でのみ、Web通信が非公開かつ変更されずに暗号化された形式で送信されます。System Managerを使用すると、ホスト管理システムのブラウザ（クライアントとして機能）とストレージシステムのコントローラ（サーバとして機能）の間の証明書を管理できます。

証明書には信頼できる認証局が署名した証明書と自己署名の証明書があります。「署名」とは、第三者が所有者のIDを検証し、そのデバイスが信頼できると判断したことを意味します。ストレージアレイの各コントローラには、自動生成された自己署名証明書が付属しています。自己署名証明書を引き続き使用することも、CA署名証明書を取得してコントローラとホストシステム間のよりセキュアな接続を確立することもできます。

> CA署名証明書はセキュリティ保護を強化しますが（中間者攻撃を阻止するなど）、大規模なネットワークの場合はコストがかかる可能性があります。一方、自己署名証明書の方が安全性は低くなりますが、無料です。したがって、自己署名証明書は本番環境ではなく内部テスト環境で最もよく使用されます。

署名済み証明書

署名済み証明書は、信頼できる第三者機関である認証局（CA）によって検証されます。署名済み証明書には、エンティティ（通常、サーバまたはWebサイト）の所有者に関する詳細、証明書の問題 および有効期限、エンティティの有効なドメイン、およびアルファベットと数字で構成されるデジタル署名が含まれています。

ブラウザを開いてWebアドレスを入力すると、証明書チェックプロセスがバックグラウンドで実行され、有効なCA署名証明書を含むWebサイトに接続しているかどうかが確認されます。通常、署名済み証明書で保護されたサイトのアドレスには、鍵のアイコンとhttpsの指定が含まれています。CA署名証明書が含まれていないWebサイトに接続しようとすると、サイトがセキュアでないことを示す警告がブラウザに表示されます。

CAは、アプリケーションプロセス中に自分の身元を確認するための手順を実行します。登録済みの会社にEメールを送信し、会社の住所を確認して、HTTPまたはDNSの検証を実行する場合があります。アプリケーションプロセスが完了すると、ホスト管理システムにロードするデジタルファイルがCAから送信されます。通常、これらのファイルには次のような信頼チェーンが含まれます。

- ルート—階層の最上位にあるのはルート証明書です。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワークデバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。
- 中間—ルートからの分岐は中間証明書ですCAは、保護されたルート証明書とサーバ証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。
- サーバー—チェーンの下部にあるサーバー証明書は、Webサイトやその他のデバイスなど、特定のエンティティを識別するサーバー証明書です。ストレージアレイの各コントローラには個別のサーバ証明書が必要です。

自己署名証明書

ストレージアレイの各コントローラには、自己署名証明書が事前にインストールされています。自己署名証明書はCA署名証明書と似ていますが、第三者ではなくエンティティの所有者によって検証される点が異なります。CA署名証明書と同様に、自己署名証明書には独自の秘密鍵が含まれており、サーバとクライアントの間のHTTPS接続を介してデータが暗号化および送信されることも保証されます。ただし、自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しません。

自己署名証明書はブラウザでは「信頼されている」ものではありません。自己署名証明書のみを含むWebサイトに接続しようとするたびに、ブラウザに警告メッセージが表示されます。Webサイトに進むには、警告メッセージ内のリンクをクリックする必要があります。これにより、基本的には自己署名証明書が受け入れられます。

キー管理サーバに使用する証明書

ドライブセキュリティ機能を持つ外部キー管理サーバを使用している場合は、そのサーバとコントローラの間の認証用の証明書を管理することもできます。

証明書の用語

証明書管理に関連する用語を次に示します。

期間	説明
できます	認証局（CA）は、インターネットセキュリティのためにデジタル証明書と呼ばれる電子文書を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバの間のセキュアな接続が確立されます。
CSR	証明書署名要求（CSR）は、申請者から認証局（CA）に送信されるメッセージです。CSRは、CAが証明書の問題 に必要な情報を検証します。
証明書	証明書はセキュリティ上の目的でサイトの所有者を識別するもので、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明（署名）する信頼されたエンティティのIDが含まれます。
証明書チェーン	証明書にセキュリティレイヤを追加するファイルの階層。通常、チェーンの最上位にはルート証明書が1つ、中間証明書が1つ以上、エンティティを識別するサーバ証明書が1つ含まれます。
クライアント証明書	セキュリティキー管理のために、クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバがコントローラのIPアドレスを信頼できるようにします。
中間証明書	証明書チェーンのルートから1つ以上の中間証明書が分岐します。CAは、保護されたルート証明書とサーバ証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。
キー管理サーバ証明書	セキュリティキー管理のために、キー管理サーバ証明書はサーバを検証し、ストレージアレイがサーバのIPアドレスを信頼できるようにします。

期間	説明
キーストア	キーストアはホスト管理システム上のリポジトリであり、秘密鍵とそれに対応する公開鍵および証明書が格納されています。これらのキーと証明書によって、コントローラなどの独自のエンティティが識別されます。
OCSPサーバ	Online Certificate Status Protocol（OCSP）サーバは、スケジュールされた有効期限の前に認証局（CA）が証明書を失効させたかどうかを確認し、証明書が失効している場合はユーザがサーバにアクセスできないようにします。
ルート証明書	ルート証明書は、証明書チェーンの階層の最上位にあります。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワークデバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。
署名済み証明書	認証局（CA）によって検証される証明書。このデータファイルには秘密鍵が含まれており、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、署名済み証明書には、エンティティ（通常、サーバまたはWebサイト）の所有者に関する詳細およびアルファベットと数字で構成されるデジタル署名が含まれています。署名済み証明書は信頼チェーンを使用するため、本番環境で最もよく使用されます。「CA署名証明書」または「管理証明書」とも呼ばれます。
自己署名証明書	自己署名証明書は、エンティティの所有者によって検証されます。このデータファイルには秘密鍵が含まれており、サーバとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、アルファベットと数字で構成されるデジタル署名も含まれます。自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しないため、テスト環境で最もよく使用されます。「事前にインストールされている」証明書とも呼ばれます。
サーバ証明書	サーバ証明書は、証明書チェーンの最下位にあります。Webサイトやその他のデバイスなど、特定のエンティティを識別します。ストレージシステムの各コントローラには個別のサーバ証明書が必要です。

方法

コントローラの**CA**署名証明書を使用する

コントローラとSystem Managerへのアクセスに使用されるブラウザとの間のセキュアな通信を確立するために、CA署名証明書を取得できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。

このタスクについて

CA署名証明書の使用は、3つの手順で構成される手順 です。

手順**1**：コントローラの**CSR**を作成および送信します

最初にストレージアレイの各コントローラの証明書署名要求（CSR）ファイルを生成し、そのファイルを認証局（CA）に送信する必要があります。

作業を開始する前に

- 各コントローラのIPアドレスまたはDNS名を確認しておく必要があります。

このタスクについて

CSRは、組織に関する情報、コントローラのIPアドレスまたはDNS名、およびコントローラのWebサーバを識別するキーペアを提供します。このタスクでは、ストレージアレイにコントローラが1つしかない場合はCSRファイルが1つ、コントローラが2つある場合は2つ生成されます。

> CAに送信したあとで新しいCSRを生成しないでください。CSRの生成時に、システムでは秘密鍵と公開鍵のペアが作成されます。公開鍵はCSRの一部であり、秘密鍵はキーストアに保持されます。署名済み証明書を受け取ってキーストアにインポートすると、システムでは秘密鍵と公開鍵の両方が元のペアになります。そのため、CSRをCAに送信したあとで新しいCSRを生成しないでください。新しいキーを生成すると、コントローラではCAから受け取った証明書が機能しなくなります。

手順

1. **[**]メニューを選択します。**[**設定**][**証明書**]**。
2. [アレイ管理]タブで、[* CSR全体*]を選択します。

   > 2台目のコントローラの自己署名証明書を受け入れるよう求めるダイアログボックスが表示された場合は、*自己署名証明書を受け入れる*をクリックして続行します。

3. 次の情報を入力し、[次へ*]をクリックします。
   - 組織--会社または組織の正式名称。Inc.やCorp.などの接尾辞も含めて入力してください
   - 組織単位（オプション）--証明書を処理している組織の部門。
   - 市区町村--ストレージアレイまたは事業の所在地である市区町村。
   - 都道府県（オプション）-ストレージアレイまたは事業の所在地である都道府県。
   - 国の**ISO**コード--自国を表す2桁のISO（国際標準化機構）コード（USなど）。

   > 一部のフィールドには、コントローラのIPアドレスなどの適切な情報があらかじめ入力されています。事前入力された値は、明らかな間違いでないかぎり変更しないでください。たとえば、CSRをまだ作成していない場合、コントローラのIPアドレスは「localhost」に設定されます。 この場合は、「localhost」をコントローラのDNS名またはIPアドレスに変更する必要があります。

4. ストレージアレイ内のコントローラAに関する次の情報を確認または入力します。
   - コントローラ**A**の共通名--コントローラAのIPアドレスまたはDNS名がデフォルトで表示されますこのアドレスが正しいことを確認してください。ブラウザでSystem Managerにアクセスする際に入力したアドレスと正確に一致している必要があります。
   - コントローラ**A**の代替**IP**アドレス-共通名がIPアドレスの場合は、コントローラAの追加のIPアドレスまたはエイリアスをオプションで入力できます複数指定する場合は、カンマで区切って入力します。

- コントローラ**A**の代替**DNS**名--共通名がDNS名の場合は、コントローラAの追加のDNS名を入力します複数指定する場合は、カンマで区切って入力します。代替DNS名がない場合は、最初のフィールドに入力したDNS名をここにコピーします。ストレージアレイにコントローラが1台しかない場合は、「完了」ボタンを使用できます。ストレージアレイにコントローラが2台ある場合は、* Next *ボタンを使用できます。

> CSR要求を最初に作成するときは、[この手順をスキップ]リンクをクリックしないでください。このリンクは、エラーからリカバリする場合に使用します。CSR要求が一方のコントローラで失敗し、もう一方のコントローラで失敗することがあります。このリンクを使用すると、コントローラAでCSRがすでに定義されている場合はその作成をスキップし、コントローラBでCSRを再作成する次の手順に進むことができます

5. コントローラが1台しかない場合は、[完了]をクリックします。コントローラが2台ある場合は、[次へ]をクリックしてコントローラBの情報を入力し（上記と同じ）、[完了]をクリックします。

   シングルコントローラの場合は、1つのCSRファイルがローカルシステムにダウンロードされます。デュアルコントローラの場合は、2つのCSRファイルがダウンロードされます。ダウンロードフォルダの場所は、ブラウザによって異なります。

6. ダウンロードしたCSRファイルの場所を確認します。フォルダの場所はブラウザによって異なります。
7. CSRファイルをCAに送信し、PEM形式の署名済み証明書を要求します。
8. CAから証明書が返されるまで待ってから、に進みます [手順2：コントローラの署名済み証明書をインポートする]。

手順**2**：コントローラの署名済み証明書をインポートする

署名済み証明書を受け取ったあと、コントローラのファイルをインポートします。

作業を開始する前に

- 署名済み証明書ファイルをCAから受け取っておきます。
- ファイルがローカルシステム上にある必要があります。
- CAからチェーン証明書（たとえば、.p7bファイル）が提供された場合は、チェーンファイルを個々のファイル（ルート証明書、1つ以上の中間証明書、コントローラを識別するサーバ証明書）に展開する必要があります。Windowsのcertmgrユーティリティーを使用してファイルを展開できます(右クリックして[**menu: All Tasks[Export]**)を選択します)エクスポートが完了すると、チェーン内の証明書ファイルごとに1つのCERファイルが表示されます。

このタスクについて

このタスクでは、証明書ファイルをアップロードする方法について説明します。

手順

1. **[**]メニューを選択します。**[**設定**][**証明書**]**。
2. [* Array Management*（アレイ管理*）]タブで、[* Import*（インポート*）]を選択し

   証明書ファイルをインポートするためのダイアログボックスが表示されます。

3. 「*参照」ボタンをクリックして、最初にルートファイルと中間ファイルを選択してから、コントローラの各サーバ証明書を選択します。ルートファイルと中間ファイルは両方のコントローラで同じです。サーバ証明書のみコントローラごとに一意です。

ファイル名がダイアログボックスに表示されます。

4. [* インポート *] をクリックします。

   ファイルがアップロードされて検証されます。

結果

セッションは自動的に終了します。証明書を有効にするには、再度ログインする必要があります。再度ログインすると、新しいCA署名証明書がセッションに使用されます。

管理証明書をリセットします

コントローラの証明書をCA署名証明書から工場出荷時の自己署名証明書に戻すことができます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- CA署名証明書を事前にインポートしておく必要があります。

このタスクについて

リセット機能は、現在のCA署名証明書ファイルを各コントローラから削除します。その後、コントローラでは自己署名証明書が再び使用されるようになります。

手順

1. **[]**メニューを選択します。**[**設定**][**証明書**]**。
2. [* Array Management*（アレイ管理）]タブで、[* Reset*（リセット）]を選択します。

   Confirm * Reset Management Certificates *ダイアログボックスが開きます。

3. フィールドに「reset」と入力し、「* Reset *」をクリックします。

   ブラウザをリフレッシュすると、デスティネーションサイトへのアクセスがブロックされ、サイトでHTTP Strict Transport Securityが使用されていると報告されることがあります。この状況は、自己署名証明書に切り替えると発生します。デスティネーションへのアクセスをブロックしている状態をクリアするには、ブラウザから参照データをクリアする必要があります。

結果

コントローラでは自己署名証明書が再び使用されるようになります。そのため、セッションの自己署名証明書を手動で承認するように求められます。

インポートされた証明書の情報を表示

証明書ページでは、ストレージアレイの証明書タイプ、発行元、および有効な証明書の日付範囲を確認できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。

手順

1. メニューから[設定][証明書]を選択します。
2. いずれかのタブを選択して、証明書に関する情報を表示します。

タブをクリックする	説明
アレイ管理	ルートファイル、中間ファイル、サーバファイルなど、各コントローラ用にインポートしたCA署名証明書に関する情報が表示されます。
高い信頼性	コントローラ用にインポートしたその他すべてのタイプの証明書に関する情報が表示されます。[Show certificates that are …]の下のフィルタフィールドを使用して、ユーザがインストールした証明書または事前にインストールされた証明書を表示します。 • ユーザーがインストールしたもの。ユーザがストレージアレイにアップロードした証明書。信頼された証明書（コントローラがサーバではなくクライアントとして機能する場合）、LDAPS証明書、アイデンティティフェデレーション証明書が含まれます。 • プリインストール。ストレージアレイに付属の自己署名証明書。
キー管理	外部キー管理サーバ用にインポートしたCA署名証明書に関する情報が表示されます。

クライアントとして機能するコントローラの証明書をインポートする

コントローラがネットワークサーバの信頼チェーンを検証できないために接続を拒否した場合は、[信頼済み]タブから証明書をインポートできます。このタブでは、コントローラ（クライアントとして動作）がそのサーバからの通信を受け入れることができます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 証明書ファイルがローカルシステムにインストールされている必要があります。

このタスクについて

別のサーバがコントローラ（LDAPサーバやTLSを使用するsyslogサーバなど）に接続できるようにするには、[信頼済み]タブから証明書をインポートする必要があります。

手順

1. **[**]メニューを選択します。**[**設定**][**証明書**]**。
2. [**Trusted**]タブで、[**Import**]を選択します。

   信頼された証明書ファイルをインポートするためのダイアログボックスが表示されます。

3. Browse（参照）*をクリックして、コントローラの証明書ファイルを選択します。

   ダイアログボックスにファイル名が表示されます。

4. [* インポート *] をクリックします。

結果

ファイルがアップロードされて検証されます。

証明書失効チェックを有効にします

失効した証明書の自動チェックを有効にして、Online Certificate Status Protocol（OCSP）サーバがユーザによるセキュアでない接続をブロックするようにすることができます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 両方のコントローラにDNSサーバが設定されている必要があります。これにより、OCSPサーバの完全修飾ドメイン名が使用できるようになります。このタスクはハードウェアページから実行できます。
- 独自のOCSPサーバを指定する場合は、そのサーバのURLを確認しておく必要があります。

このタスクについて

自動失効チェックは、CAが発行した証明書に問題がある場合や、秘密鍵が漏えいした場合に役立ちます。

このタスクでは、OCSPサーバを設定するか、証明書ファイルに指定されているサーバを使用することができます。OCSPサーバは、スケジュールされた有効期限よりも前にCAによって失効された証明書がないかを判断し、証明書が失効している場合は、ユーザによるサイトへのアクセスをブロックします。

手順

1. **[**]メニューを選択します。**[**設定**][**証明書**]**。
2. [**Trusted**]タブを選択します。

   また、*Key Management*タブから失効チェックを有効にすることもできます。

3. [一般的でないタスク]をクリックし、ドロップダウンメニューから[失効チェックを有効にする*]を選択します。
4. 「失効チェックを有効にする」を選択して、チェックボックスにチェックマークが表示され、ダイアログボックスに追加のフィールドが表示されるようにします。
5. [* OCSPレスポンダのアドレス*]フィールドに、OCSPレスポンダサーバのURLをオプションで入力できます。アドレスを入力しない場合は、証明書ファイルで指定されているOCSPサーバのURLが使用されます。
6. [アドレスのテスト*]をクリックして、指定したURLへの接続をシステムがオープンできることを確認します。
7. [保存（ Save ）] をクリックします。

結果

証明書が失効しているサーバにストレージアレイが接続しようとすると、接続は拒否され、イベントがログに記録されます。

信頼された証明書を削除する

以前に[信頼済み]タブからインポートした、ユーザーがインストールした証明書を削除できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 信頼された証明書を新しいバージョンに更新する場合は、古い証明書を削除する前に更新された証明書をインポートする必要があります。

> コントローラとLDAPサーバなどの別のサーバの認証に使用している証明書を新しい証明書をインポートする前に削除すると、システムにアクセスできなくなることがあります。

このタスクについて

このタスクでは、ユーザがインストールした証明書を削除する方法について説明します。あらかじめインストールされている自己署名証明書を削除することはできません。

手順

1. **[**]メニューを選択します。**[**設定**][**証明書**]**。
2. [**Trusted**]タブを選択します。

   ストレージアレイの信頼された証明書が表に表示されます。

3. 削除する証明書を表から選択します。
4. [*]メニューの[一般的ではないタスク[削除]*をクリックします

   [信頼された証明書の削除の確認]ダイアログボックスが開きます。

5. フィールドに「delete」と入力し、「* Delete *」をクリックします。

キー管理サーバでの認証に**CA**署名証明書を使用する

キー管理サーバとストレージアレイコントローラの間のセキュアな通信を確立するためには、適切な証明書セットを設定する必要があります。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。

このタスクについて

コントローラとキー管理サーバ間の認証は、2段階の手順 です。

手順1：キー管理サーバを使用した認証用にCSRを作成および送信します

最初に証明書署名要求（CSR）ファイルを生成し、そのCSRを使用して、キー管理サーバで信頼されている認証局（CA）から署名済みのクライアント証明書を要求する必要があります。ダウンロードしたCSRファイルを使用して、キー管理サーバからクライアント証明書を作成およびダウンロードすることもできます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。

このタスクについて

このタスクでは、CSRファイルを生成する方法について説明します。生成したファイルを使用して、キー管理サーバで信頼されるCAから署名済みのクライアント証明書を要求します。クライアント証明書は、キー管理サーバが自身のKey Management Interoperability Protocol（KMIP）要求を信頼できるよう、ストレージアレイのコントローラを検証します。このタスクでは、組織に関する情報を指定する必要があります。

手順

1. **[]**メニューを選択します。**[設定][証明書]**。
2. [キー管理]タブで、[* CSR全体*]を選択します。
3. 次の情報を入力します。
   - 共通名--証明書ファイルに表示されるストレージアレイ名など、このCSRを識別する名前。
   - 組織--会社または組織の正式名称。Inc.やCorp.などの接尾辞も含めて入力してください
   - 組織単位（オプション）--証明書を処理している組織の部門。
   - 市区町村--組織の所在地である市区町村。
   - 都道府県**(**オプション**)**--組織の所在地である都道府県。
   - 国の**ISO**コード--組織の所在地である米国などの2桁のISO（国際標準化機構）コード。
4. [* ダウンロード] をクリックします。

   CSRファイルがローカルシステムに保存されます。

5. キー管理サーバで信頼されているCAから署名済みのクライアント証明書を要求します。
6. クライアント証明書がある場合は、に進みます [手順2：キー管理サーバの証明書をインポートする]。

手順2：キー管理サーバの証明書をインポートする

次の手順として、ストレージアレイとキー管理サーバの間の認証用に証明書をインポートします。証明書には2種類あります。クライアント証明書はストレージアレイのコントローラを検証し、キー管理サーバ証明書はサーバを検証します。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 署名済みのクライアント証明書ファイルがある（を参照） 手順1：キー管理サーバを使用した認証用にCSRを作成および送信します）をクリックし、System Managerにアクセスするホストにファイルをコピーしておきます。クライアント証明書は、キー管理サーバが自身のKey Management Interoperability Protocol（KMIP）要求を信頼できるよう、ストレージアレイのコントローラを検証します。

- キー管理サーバからサーバ証明書ファイルを取得し、そのファイルをSystem Managerにアクセスするホストにコピーする必要があります。キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。

> サーバ証明書の詳細については、キー管理サーバのドキュメントを参照してください。

このタスクについて

このタスクでは、ストレージアレイコントローラとキー管理サーバの間の認証用に証明書ファイルをアップロードする方法について説明します。コントローラのクライアント証明書ファイルとキー管理サーバのサーバ証明書ファイルの両方をロードする必要があります。

手順

1. **[**]メニューを選択します。**[**設定**][**証明書**]**。
2. [キー管理]タブで、[インポート]を選択します。

   証明書ファイルをインポートするためのダイアログボックスが表示されます。

3. Select client certificate の横にある Browse *ボタンをクリックして、ストレージアレイのコントローラ用のクライアント証明書ファイルを選択します。

   ダイアログボックスにファイル名が表示されます。

4. キー管理サーバのサーバ証明書の選択*の横にある*参照*ボタンをクリックして、キー管理サーバのサーバ証明書ファイルを選択します。

   ダイアログボックスにファイル名が表示されます。

5. [* インポート *] をクリックします。

   ファイルがアップロードされて検証されます。

キー管理サーバ証明書をエクスポートする

キー管理サーバ用の証明書をローカルマシンに保存できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、証明書の機能は表示されません。
- 証明書をインポートしておく必要があります。

手順

1. **[**]メニューを選択します。**[**設定**][**証明書**]**。
2. [キー管理（Key Management *）]タブを選択します。
3. 表からエクスポートする証明書を選択し、* Export *（エクスポート）をクリックします。

   [保存（Save）]ダイアログボックスが開きます。

4. ファイル名を入力し、*保存*をクリックします。

よくある質問です

Cannot Access Other Controllerダイアログボックスが表示されるのはなぜですか。

CA証明書に関連する特定の処理（証明書のインポートなど）を実行すると、2台目のコントローラの自己署名証明書を受け入れるよう求めるダイアログボックスが表示されることがあります。

2台のコントローラを搭載したストレージアレイ（デュプレックス構成）では、SANtricity System Managerが2台目のコントローラと通信できない場合、または処理の特定の段階でブラウザが証明書を受け入れられない場合に、このダイアログボックスが表示されることがあります。

このダイアログボックスが表示された場合は、[自己署名証明書を承認する]をクリックして続行します。パスワードの入力を求めるダイアログボックスが表示された場合は、System Managerへのアクセスに使用する管理者パスワードを入力します。

このダイアログボックスが再び表示され、証明書のタスクを完了できない場合は、次のいずれかの手順を実行してください。

- 別のブラウザを使用してこのコントローラにアクセスし、証明書を受け入れて続行します。
- System Managerを使用して2台目のコントローラにアクセスし、自己署名証明書を受け入れてから、1台目のコントローラに戻って続行します。

外部キー管理を行うために**System Manager**にアップロードする必要がある証明書を確認するにはどうすればよいですか？

外部キー管理では、ストレージアレイとキー管理サーバが互いに信頼関係を確立できるように、2つのエンティティの間の認証用に2種類の証明書をインポートします。

クライアント証明書は、キー管理サーバが自身のKey Management Interoperability Protocol（KMIP）要求を信頼できるよう、ストレージアレイのコントローラを検証します。クライアント証明書を取得するには、System Managerを使用してストレージアレイのCSRを作成します。その後、CSRをキー管理サーバにアップロードし、そこからクライアント証明書を生成できます。クライアント証明書を作成したら、System Managerにアクセスしているホストにそのファイルをコピーします。

キー管理サーバ証明書は、ストレージアレイがサーバのIPアドレスを信頼できるよう、キー管理サーバを検証します。キー管理サーバからサーバ証明書ファイルを取得し、System Managerにアクセスするホストにそのファイルをコピーします。

証明書失効チェックについて、どのような点に注意する必要がありますか？

System Managerでは、証明書失効リスト（CRL）をアップロードする代わりに、Online Certificate Status Protocol（OCSP）サーバを使用して失効した証明書をチェックできます。

失効した証明書は信頼しないようにしてください。証明書が失効する理由はいくつかあります。たとえば、認証局（CA）から証明書が適切に発行されていない、秘密鍵が不正に使用された、特定されたエンティティが

ポリシーの要件を満たしていない、などの場合です。

System ManagerでOCSPサーバへの接続を確立すると、ストレージアレイは、AutoSupport サーバ、外部キー管理サーバ（EKMS）、Lightweight Directory Access Protocol over SSL（LDAPS）サーバ、またはsyslogサーバに接続するたびに失効チェックを実行します。ストレージアレイは、これらのサーバの証明書の検証を試行して、証明書が失効していないことを確認します。その証明書について、サーバから「good」、「revoked」「unknown」のいずれかの値が返されます。証明書が失効している場合や、アレイがOCSPサーバにアクセスできない場合は、接続が拒否されます。

> System ManagerまたはコマンドラインインターフェイスCLI）で指定したOCSPレスポンダアドレスは、証明書ファイル内のOCSPアドレスよりも優先されます。

失効チェックが有効になるのはどのタイプのサーバですか？

ストレージアレイは、AutoSupport サーバ、外部キー管理サーバ（EKMS）、Lightweight Directory Access Protocol over SSL（LDAPS）サーバ、またはsyslogサーバに接続するたびに失効チェックを実行します。