



## 証明書管理 SANtricity 11.6

NetApp  
February 12, 2024

# 目次

- 証明書管理 ..... 1
  - 概念 ..... 1
  - 方法 ..... 3

# 証明書管理

## 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。

### 署名済み証明書

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。Unified Managerを使用すると、ホスト管理システムのブラウザおよび検出されたストレージレイのコントローラ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を確認されます。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。
- \*Intermediate \*-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証明書です。ストレージ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。

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。

## Unified Managerの証明書

Unified Managerインターフェイスは、ホストシステムにWeb Services Proxyとともにインストールされます。ブラウザを開いてUnified Managerに接続しようすると、ホストが信頼できるソースであるかどうかを確認するためにデジタル証明書がチェックされます。ブラウザでサーバのCA署名証明書が見つからない場合は、警告メッセージが表示されます。そこからWebサイトにアクセスして、そのセッションの自己署名証明書を受け入れることができます。または、CAから署名入りのデジタル証明書を取得して、警告メッセージが表示されないようにすることもできます。

## コントローラの証明書

Unified Managerセッション中に、CA署名証明書のないコントローラにアクセスしようすると、追加のセキュリティメッセージが表示されることがあります。この場合、自己署名証明書を永続的に信頼するか、コントローラのCA署名証明書をインポートして、Web Services Proxyサーバがこれらのコントローラから受信するクライアント要求を認証できるようにすることができます。

## 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。                             |

| 期間                          | 説明  |
|-----------------------------|---|
| 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。   |
| 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。   |
| 信頼ストア                       | 信頼ストアは、CAなどの信頼できるサードパーティの証明書を格納するリポジトリです。   |
| Web Services Proxyの使用<br>方法 | Web Services Proxyは標準のHTTPSメカニズムによるアクセスを提供するプロキシで、管理者にストレージレイの管理サービスの設定を許可します。このプロキシは、WindowsホストまたはLinuxホストにインストールできます。Unified ManagerインターフェイスにはWeb Services Proxyが付随しています。   |

## 方法

### CA署名証明書を使用する

Unified Managerをホストする管理システムへのセキュアなアクセスを確立するために、CA署名証明書を取得してインポートできます。

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、2つの手順で構成された手順 です。

#### 手順1：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、そのファイルをCAに送信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

このタスクでは、Unified ManagerとWeb Services Proxyをホストするシステムの署名付き管理証明書を受け取るためにCAに送信するCSRファイルを生成する方法について説明します。組織に関する情報とともに、ホストシステムのIPアドレスまたはDNS名を指定する必要があります。



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. [証明書管理]を選択します。
2. [管理（Management）]タブで、[CSR全体\*（\* Complete CSR \*）]を選択します。
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--ホストシステム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)--ホストシステム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）。
4. ホストシステムに関する次の情報を入力します。
  - 共通名-- WebサービスプロキシがインストールされているホストシステムのIPアドレスまたはDNS名。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Unified 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。http://またはhttps://を含めないでください。
  - 代替IPアドレス--共通名がIPアドレスの場合は'オプションでホストシステムの追加のIPアドレスまたはエイリアスを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。
  - 代替DNS名--共通名がDNS名の場合は'ホストシステムの追加の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。

5. [完了] をクリックします。

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。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. CSRファイルをCAに送信し、PEM形式またはDER形式の署名済み証明書を要求します。

完了後

CAから証明書ファイルが返されるまで待ってから、に進みます **"手順2：管理証明書をインポートする"**。

手順2：管理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、Unified Managerインターフェイスがインストールされているホストシステムの証明書チェーンをインポートします。

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。
- 証明書署名要求（CSRファイル）を生成してCAに送信しておきます。
- 信頼された証明書ファイルをCAから受け取っておきます。
- 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。
- 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、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。

手順

1. [証明書管理]を選択します。
2. [管理（Management）]タブで、[インポート（Import）]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. [**Browse**](参照)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、次にサーバ証明書を選択します。

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。

結果

ファイルがアップロードされて検証されます。証明書の情報は、証明書の管理ページに表示されます。

管理証明書をリセットします

管理証明書を工場出荷時の自己署名証明書の状態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。

このタスクについて

このタスクでは、WebサービスプロキシとSANtricity Unified Managerがインストールされているホストシステムから現在の管理証明書を削除します。証明書をリセットすると、ホストシステム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. [証明書管理]を選択します。
2. [管理（Management）]タブで、[リセット（Reset）]を選択します。

[管理証明書のリセットの確認]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

システムでサーバの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。

## アレイの証明書をインポートします

必要に応じて、SANtricity Unified Managerをホストするシステムで認証できるように、ストレージアレイの証明書をインポートすることができます。証明書には、認証局（CA）が署名した証明書と自己署名の証明書があります。

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。
- 信頼された証明書をインポートする場合は、SANtricity System Managerを使用してストレージアレイのコントローラの証明書をインポートする必要があります。

手順

1. [証明書管理]を選択します。
2. [Trusted]タブを選択します。

このページには、ストレージアレイについて報告されたすべての証明書が表示されます。

3. CA証明書をインポートするには\* MENU：Import を選択し、自己署名証明書をインポートするには MENU：Import [Self-Signed storage array certificates]\*を選択します。

表示を制限するには、[\*次の証明書を表示...]フィルタリングフィールドを使用するか、いずれかの列見出



しをクリックして証明書の行をソートします。

4. ダイアログボックスで証明書を選択し、\*インポート\*をクリックします。

証明書がアップロードされて検証されます。

## 証明書を表示します

証明書を使用している組織、証明書を発行した機関、有効期間、フィンガープリント（一意の識別子）など、証明書の概要情報を表示できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロフィー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. [証明書管理]を選択します。
2. 次のいずれかのタブを選択します。
  - 管理-- Webサービスプロキシをホストするシステムの証明書を表示します。管理証明書には、自己署名の証明書と認証局（CA）によって承認された証明書があります。この証明書によって、Unified Managerへのセキュアなアクセスが許可されます
  - \* Trusted \*-- Unified ManagerがストレージレイやLDAPサーバなどのその他のリモートサーバにアクセスできる証明書を表示します認証局（CA）から発行された証明書と自己署名の証明書が含まれます。
3. 証明書の詳細を表示するには、その行を選択し、行の最後にある省略記号を選択して、\*表示\*または\*エクスポート\*をクリックします。

## 証明書をエクスポートします

証明書をエクスポートして詳細を確認することができます。

作業を開始する前に

エクスポートしたファイルを開くには、証明書ビューアアプリケーションが必要です。

手順

1. [証明書管理]を選択します。
2. 次のいずれかのタブを選択します。
  - 管理-- Webサービスプロキシをホストするシステムの証明書を表示します。管理証明書には、自己署名の証明書と認証局（CA）によって承認された証明書があります。この証明書によって、Unified Managerへのセキュアなアクセスが許可されます
  - \* Trusted \*-- Unified ManagerがストレージレイやLDAPサーバなどのその他のリモートサーバにアクセスできる証明書を表示します認証局（CA）から発行された証明書と自己署名の証明書が含まれます。
3. 証明書をページから選択し、行の最後にある省略記号をクリックします。
4. [\* Export\*]をクリックし、証明書ファイルを保存します。

5. 証明書ビューアアプリケーションでファイルを開きます。

## 信頼された証明書を削除する

期限切れになった証明書など、不要になった証明書を削除することができます。

作業を開始する前に

古い証明書を削除する前に、新しい証明書をインポートしてください。



ルート証明書または中間証明書を削除すると、同じ証明書ファイルが共有されている可能性があるため、複数のストレージレイに影響する可能性があります。

手順

1. [証明書管理]を選択します。
2. [Trusted]タブを選択します。
3. テーブルで1つ以上の証明書を選択し、\*削除\*をクリックします。



◦ Delete \*機能は、プリインストールされている証明書では使用できません。

[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。

4. 削除を確認し、\* Delete \*をクリックします。

証明書がテーブルから削除されます。

## 信頼されていない証明書を

信頼されていない証明書の問題は、ストレージレイからSANtricity Unified Managerへのセキュアな接続を確立しようとしたときに、接続がセキュアであることが確認できないと発生します。証明書ページでは、信頼されていない証明書を解決するために、ストレージレイから自己署名証明書をインポートするか、信頼できる第三者機関から発行された認証局（CA）証明書をインポートします。

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。
- CA署名証明書をインポートする場合は、次の点に注意してください。
  - ストレージレイの各コントローラの証明書署名要求（.CSRファイル）を生成してCAに送信しておく必要があります。
  - 信頼された証明書ファイルをCAから受け取っておきます。
  - 証明書ファイルがローカルシステム上にある必要があります。

このタスクについて

信頼された追加のCA証明書のインストールが必要になる可能性があるのは、次のいずれかに該当する場合です。

- ストレージアレイを新たに追加した。
- 一方または両方の証明書の期限が切れている。
- 一方または両方の証明書が失効している。
- 一方または両方の証明書のルート証明書または中間証明書がない。

#### 手順

1. [証明書管理]を選択します。
2. **[Trusted]**タブを選択します。

このページには、ストレージアレイについて報告されたすべての証明書が表示されます。

3. いずれかの\*メニューを選択します。Import [Certificates]\*。CA証明書または\*メニューをインポートするには：[自己署名ストレージアレイ証明書]をインポートして自己署名証明書をインポートします。

表示を制限するには、[\*次の証明書を表示...]フィルタリングフィールドを使用するか、いずれかの列見出しをクリックして証明書の行をソートします。

4. ダイアログボックスで証明書を選択し、\*インポート\*をクリックします。

証明書がアップロードされて検証されます。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。